NTCA CYBERSECURITY SERIES

(Part 4)

Cyber Incident Response Plan

NTCA THE RURAL BROADBAND ASSOCIATION®

#BeCyberwise

NTCA Cybersecurity Series
(Part 4)
Cyber Incident Response Plan

Published November 2021

4121 Wilson Blvd., Suite 1000
Arlington, VA 22203
(703) 351-2000

Disclaimer: The National Telecommunications Cooperative Association d/b/a NTCA–The Rural Broadband Association ("NTCA") is offering the NTCA Cybersecurity Series and/or its individual components for general information purposes only, and nothing contained herein constitutes legal advice or opinions of any kind. You use these documents at your own risk, and you should not use any of these documents without first seeking legal and other professional advice. NTCA makes no representations or warranties, express or implied, with respect to the Cybersecurity Series, including without limitation any warranties of fitness for a particular purpose. NTCA and its affiliates (and any of their respective directors, officers, agents, contractors, interns, suppliers and employees) are not responsible for, and expressly disclaim, all liability for, damages of any kind arising out of use, reference to or reliance of any information contained within the Cybersecurity Series. Although the Cybersecurity Series may include links providing direct access to internet resources, including websites, NTCA is not responsible for the accuracy or content of information contained in these sites

Prepared by:

Womble Bond Dickinson (US) LLP, CyberESI and Telcom Insurance Group

Our goal is to:

1. Create a document that includes detailed instructions and sample language to help a small network service provider (in collaboration with its own legal and technical counsel) develop and implement a company-specific, easy-to-follow, internal, written plan for responding to and recovering from various cyber incidents.
    1. This should include, but is not limited to information on how to:
        (a) identify an incident response team;
        (b) define and categorize incident types and responses;
        (c) mitigate damages through containment, eradication and recovery strategies;
        (d) comply with internal and external notification reporting requirements;
        (e) ensure evidence is appropriately gathered and preserved;
        (f) identify outside resources; and
        (g) review and adjust to improve the plan.
2. Provide information that is consistent with the NIST Cybersecurity Framework and current law and regulation.
3. Educate small network service providers at NTCA-identified events and/or webinars about the need for cyber incident preparation and how to use the guide to develop a company-specific cyber incident response plan.

You will be presented with two items:

1. Relevant Laws, Best Practices and Standards for Your Industry Guide; and
2. Creating the Written Incident Response Plan

RELEVANT LAWS, BEST PRACTICES AND STANDARDS FOR YOUR INDUSTRY GUIDE

All businesses should map their cybersecurity spending and architecture to the data obligations in regulations, laws and contracts applicable to those specific companies. Communications companies are affected by the Federal Communications Commission (FCC), certain Federal Trade Commission (FTC) regulations[1] and requirements, standard consumer protection obligations, the restrictions of the payment card industry, and often by their commercial contracts. Beyond data network management, special operational infrastructure requirements like Supervisory Control and Data Acquisition (SCADA), a control system architecture, also complicate efforts to protect the company's information and architecture.

The good news is most of the reasoning and requirements of the various governing standards are consistent, so that progress toward meeting one standard helps with meeting the others. The bad news is that under these standards your company should be documenting all the steps it is taking to protect its systems and data. Such documentation will be important to regulators or state attorney general offices when they audit your performance. Such audits are becoming more common—often following a data breach, but sometimes initiated by whistleblowers or government investigators.

In addition to complying with applicable industry standards and legal requirements, another excellent means of reducing the risk of government fines for lax cybersecurity is to invite a third-party to analyze your company's security requirements, follow the third party's proposed steps for your company to meet these requirements, and bring your company up to speed (while documenting all the way). A third-party review shows the regulators that your company leadership has been thinking about data protection, has learned best practices and has invested in meeting them.

The FCC provides network reliability, availability and resiliency resources for rural telco providers, but it can also impose fines on providers for failures in cybersecurity. The FCC has encouraged rural telephone providers to adopt best practices recommended by the Communications Security, Reliability, and Interoperability Council (CSRIC), a federal advisory committee to the FCC,[2] to improve network reliability. These practices can help telephone companies avoid investigations or support a company's assertion of best practices should cyberattacks disable the network or expose customer information.

Specifically, cyber threat information sharing in a trusted environment enables network operators to leverage the collective knowledge, experience, and capabilities of governmental, other public, and private sources to help protect the network. As a result, the NTCA CyberShare: The Small Broadband

---

[1] As discussed below, only non-common carrier communications companies are subject to FTC regulation.

[2] FCC, Communications Security, Reliability, and Interoperability Council, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited Nov. 11, 2021).

Provider Information Sharing and Analysis Center (ISAC) provides you with immediate, actionable cyber threat information, and as an ISAC recognized by the National Council of ISACs, it is designed to maximize information flow across the small broadband provider sector and with government. CyberShare participants have access to daily and weekly reports and have the ability to communicate and collaborate in a trusted setting. **Learn about and join CyberShare**.

The FTC Act prohibits "unfair or deceptive acts or practices, in or affecting commerce." Section 5 of the FTC Act grants oversight authority to the FTC to regulate data security practices. The FTC has the authority to regulate sophisticated technologies that businesses use to protect sensitive consumer information, but the FTC Act exempts some entities from the FTC's authority, including common carriers. This common carrier exemption precludes the FTC from bringing enforcement actions against common carriers that are regulated under Title II of the Communications Act of 1934, as amended (FCC Act). Telecommunications carriers and wireless providers regulated under Title II that provide common carrier services are instead subject to FCC oversight.

Federal Data Management Oversight and ISP Regulation

The FTC and/or the FCC could be your primary federal regulator in the data privacy and cybersecurity space depending on how the political winds blow. Right now, the FTC regulates internet service providers (ISPs, and the FCC regulates telephone companies.

For the first two decades of the internet's existence, ISPs were considered to provide information services rather than telecommunications services and were therefore regulated by the FTC. During the Trump administration, ISPs were moved back under the wing of the FCC. Under the FCC's 2015 Open Internet Order, ISPs became subject to Title II common carrier regulation and were considered telecommunications carriers. The FCC also adopted a number of privacy rules in its Broadband Privacy Report and Order in the fall of 2016. These rules would have been applicable to the provision of all telecommunications services (including broadband internet access service and voice over internet protocol), and governed both data security and breach notification, but they had not been part of the regulatory regime long enough to start being enforced.

This area of law shifted again with the change in administrations in 2017, as the rules in the Broadband Privacy Report and Order were eliminated under the new Trump Administration (and new FCC leadership). The rules were initially stayed by the FCC, and then Congress passed a joint resolution repealing them entirely in April 2017. Since then, the FCC has adopted its 2017 internet Freedom Declaratory Ruling — a decision that would repeal the 2015 Open internet Order's Title II classification of broadband service and restore FTC privacy and data security oversight jurisdiction over ISPs. These rules went into effect on February 22, 2018. Later that year, the Ninth Circuit Court of Appeals made it clear that

the FTC has the right to enforce such oversight against telephone companies.

The FTC regulated ISPs for the first twenty years, and then just when the FCC was about ready to take over the task of regulating ISPs, the rules changed again and pushed such regulation back to the FTC. The FCC has always regulated telephone companies. Conceivably, if your company provides both telephone and broadband service, then either federal entity could address your treatment and protection of data and possibly fine you for violations.

The FTC has pursued many types of companies under the authority of Section 5 of the Federal Trade Commission Act, declaring that acting in opposition to published privacy policies or not protecting consumer data adequately were unfair and deceptive trade practices. The FTC claims that its charge includes requiring companies "to take affirmative steps to remediate unlawful behavior" including "implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers and provision of robust transparency and choice mechanisms to consumers." So, the FTC expects companies to be taking aggressive steps to protect consumer information.

Section 222 of the FCC Act imposes a duty on telecommunications carriers to protect the confidentiality of proprietary information of other carriers, equipment manufacturers, and customers. The FCC has historically interpreted Section 222 in the Customer Proprietary Network Information (CPNI) context, and the CPNI rules contain requirements regarding how to handle breach disclosure. The FCC has also extended CPNI rules to providers of interconnected Voice over internet Protocol (VoIP) service.

In the event of a CPNI breach, the service provider must delay customer notification until law enforcement has been notified. A CPNI breach has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

Specifically, the service provider must notify law enforcement of a breach of a customer's CPNI no later than seven business days after making a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the FBI. The FCC maintains a link to the reporting facility at **www.fcc.gov/eb/cpni**.

The service provider may notify the customer and/or disclose the breach publicly after seven business days following notification to the USSS and FBI, if the USSS and the FBI have not requested that the service provider continue to postpone disclosure. If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, that agency may direct the carrier not to disclose the breach for an initial 30-day period. This 30-day period may be extended by the law enforcement agency as reasonably necessary. The law enforcement agency must provide in writing to the service provider its initial direction and any subsequent direction.

The service provider, however, may immediately notify a customer or disclose the breach publicly after consultation with the relevant investigative agency, if the service provider believes there is an extraordinarily urgent need to notify a customer or class of customers to avoid immediate and irreparable harm. Customer breach notification is discussed later in this guide.

Service providers must maintain a record of any discovered breaches and notifications to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notifications, for a period of at least two years. This record must include, if available, the date that the service provider discovered the breach, the date the service provider notified the USSS and the FBI, a detailed description of the CPNI that was breached, and the circumstances of the breach.

On January 18, 2017 (under the previous administration), the FCC produced a white paper explaining what it expected in cybersecurity risk reduction for the companies the FCC regulated. The FCC claimed that it would be acting on the following cybersecurity risk reduction tasks (which it referred to as "Key Commission actions"):

- ***Promoting best practices***. Working with industry and external partners to develop a harmonized, rich repository of standards and best practices for cyber risk management.
- ***Making cybersecurity a forethought not an afterthought***. Promoting
- security by design efforts to incorporate cybersecurity during the development phase of new products and services and adopting rules requiring licensees for 5G wireless networks to submit a cybersecurity plan before commencing operations.
- ***Increasing situational awareness***. Strengthening our network outage and data breach reporting requirements.
- ***Improving information sharing***. Adopting real-time cyberthreat information sharing with federal partners and promoting sharing among private carriers.
- ***Establishing cybersecurity as integral to the Public Interest***. Identifying cybersecurity as a consideration of merger reviews."

The FCC, under new leadership, may or may not continue on this track, but its publications show an enthusiasm for proactive company protection of consumer privacy similar to what the FTC has demonstrated, including regulation of products and services considered part of the internet of Things.

The FCC published a security guide for small business that shows best practices with respect to several important security topics for communications companies. These tips are basic, but if followed, your company will be establishing a baseline of strong security practices, and they are concepts that can be easily followed by smaller businesses.

1. **Train employees in security principles**
   Establish basic security practices and policies for employees, such as requiring strong passwords and establish appropriate internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.
4. **Protect information, computers, and networks from cyberattacks**
   Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.
5. **Provide firewall security for your internet connection**
   A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.
6. **Create a mobile device action plan**
   Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.
7. **Make backup copies of important business data and information**
   Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly, and store the copies either offsite or in the cloud.
8. **Control physical access to your computers and create user accounts for each employee**
   Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.
9. **Secure your Wi-Fi networks**
   If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Passwords protect access to the router.
10. **Employ best practices on payment cards**
    Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to

agreements with your bank or processor. Isolate payment systems from other, less secure programs and don't use the same computer to process payments and surf the internet.

11. **Limit employee access to data and information, and limit authority to install software**
    Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs and should not be able to install any software without permission.
12. **Passwords and authentication**
    Require employees to use unique passwords and change passwords every three months. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.

In addition, The FCC prescribed best practices for the operational networks managed by rural telephone companies, including:

1. Providing back-up power at cell sites and remote equipment locations, which could be some combination of batteries, generators and/or fuel cells;
2. Pre-arranging contact information and access to restorative information with local power companies;
3. Conducting physical site audits after any major event to ensure physical integrity and orientation of hardware and software;
4. Proper oversight of third parties servicing critical network facilities.

Given rapid developments in this subject area, we urge you to contact your attorney with specific questions you may have on these issues.

State Law

Service providers should be familiar with any applicable State law on security breach notifications as the FCC's rules do not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the FCC's CPNI breach notification requirements, and then only to the extent of the inconsistency. Nearly every state has a requirement that its residents be provided with notice if those residents' personal data is lost. Most of the states define personal data as including *both* an identifying fact— like name, email, or address – plus an account number.

States also often require that if enough of their residents are affected by a data incident, then the company holding the data should send notice to state agencies, like the state police or

the attorney general's office, and/or send notice to the three major credit reporting agencies. Canada and Europe are beginning to implement similar notice requirements, but these are newer and have not been triggered or interpreted much yet. These breach notice laws, in the states and elsewhere, are complicated and ever changing. For example, some states require that the affected company send a detailed description of the data exposure incident to affected residents, while other states forbid sending a detailed description.

Check with your data security lawyer to obtain state data breach details that will provide guidance through this dangerous minefield. Your specific state requirements will need to be included in your written incident response plan.

Relevant Data Security Standards

So where is an ISP and/or telecommunications company going to find the relevant standards to follow in building its cybersecurity infrastructure? First, ask a third party that works in this area to show you what others in the industry are doing.

Homeland Security Presidential Directive 7 (HSPD-7) required the Department of Homeland Security to "...serve as the focal point for the security of cyberspace ..." with a mission that included "... analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems." This directive established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. In addition, it required heads of all federal agencies to "... develop ... plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate." Hence, the federal government began to directly address issues of cybersecurity within the federal government systems.

NRIC Best Practices

The Communications Act of 1934 charges the FCC with regulating interstate and foreign commerce in communication by wire and radio to make available to all Americans a rapid, efficient, nationwide and worldwide wireless and wireline communications services. The FCC has interpreted this to grant it power of the security of communications systems. To this end, the FCC chartered a federal advisory committee called the Network Reliability and Interoperability Council (NRIC) in 1992 to develop industry best practices to promote network reliability and interoperability, but NRIC's charge has extended to address external threats for carriers, CATV, wireless, ISPs, equipment suppliers, and systems integrators. NRIC is chaired by industry executives and populated with private company and consulting subject matter experts.

Eventually the NRIC was replaced by the Communications Security, Reliability and Interoperability Council (CSRIC), established by the FCC to address the prevention and remediation of detrimental cyber events, the development of best practices to improve overall communications reliability, the availability and performance of communications services and emergency alerting during natural disasters, terrorist attacks, cybersecurity attacks or other events that result in exceptional strain

on the communications infrastructure, the rapid restoration of communications services in the event of widespread or major disruptions, and the steps communications providers can take to help secure end-users and servers.

CSRIC has issued recent recommendations on best practices for physical security, cybersecurity, public safety and disaster recovery. CSRIC's work on cybersecurity was conducted by leading network operators from the communications sector and resulted in over 200 best practices to help service providers secure their networks against accidental events and criminal activities. CSRIC cybersecurity best practices can be categorized into four basic areas: (1) updating software; (2) secure equipment management; (3) intrusion prevention and detection; and (4) intrusion analysis and response. More specifically, CSRIC Working Group 2A recommends a set of 397 Best Practices across 9 focus areas (Wireless, IP Services, Network, People, Legacy services, Identity Management, Encryption, Vulnerability Management, and Incident Management) to the FCC for consideration of adopting the best practices for general use by industry. The theory behind these best practices is that prevention of a cyberattack is cheaper that remediating the network when an attack occurs.

The detailed set of best practices for communications infrastructure is too voluminous to provide in this document and can be reached by the link in the resources section of this guide. In reduced and relevant part, the best practices for your industry include taking the following broadly defined steps:

6-6-8000 Disable Unnecessary Services when practical (e.g., Network Time Protocol (NTP), Remote Procedure Calls (RPC), Finger, Rsh-type commands, etc.)
6-6-8008 Network Architecture Isolation/Partitioning
6-6-8015 Segmenting Management Domains
6-6-8020 Security HyperPatching
6-6-8032 Patching Practices
6-6-8034 Software Patching Policy
6-6-8037 System Inventory Maintenance
6-6-8039 Patch/Fix Verification
6-6-8041 Prevent Network Element Resource Saturation
6-6-8071 Threat Awareness
6-6-8074 Denial of Service Attack – Target
6-6-8093 Validate source addresses

As an illustration, here are some of the best practices that the CSRIC holds to be critical in nature (as opposed to Important or Highly Important).

- Network Operators and Service Providers should develop processes or plans to quickly account for all employees (e.g. field techs) in or near the impact area of a disaster.
- Network Operators, Service Providers and Equipment Suppliers should establish and maintain (or contract for) a 24/7 emergency call center for internal communications. Ensure staff at this center has access to all documentation pertinent to emergency response and up-to-date call lists to notify appropriate personnel. The number to this call center should be appropriately published so personnel know where to report information.
- Network Operators and Service Providers (e.g., satellite operators) should maintain access to a back-up or secondary "uplink site" to provide tracking, telemetry and control (T.T.&C.) support for all operational communications spacecraft. The back-up or secondary site must be geographically diverse from the primary uplink facility, active and tested on some regular schedule to insure readiness and timely response.
- Network Operators, Service Providers and Equipment Suppliers should control or disable all administrative access ports (e.g., manufacturer) into R&D or production systems (e.g., remap access ports, require callback verification, add second level access gateway).
- Scanning Operations, Administration, Management and Provisioning (OAM&P) Infrastructure: Network Operators and Service Providers should regularly scan infrastructure for vulnerabilities/exploitable conditions. Operators should understand the operating systems and applications deployed on their network and keep abreast of vulnerabilities, exploits, and patches.
- Distribution of Encryption Keys: When Network Operators, Service Providers and Equipment Suppliers use an encryption technology in the securing of network equipment and transmission facilities, cryptographic keys must be distributed using a secure protocol that: a) ensures the authenticity of the recipient, b) does not depend upon secure transmission facilities, and c) cannot be emulated by a non-trusted source.
- Validate Source Addresses: Service Providers should validate the source address of all traffic sent from the customer for which they provide internet access service and block any traffic that does not comply with expected source addresses. Service Providers typically assign customers addresses from their own address space, or if the customer has their own address space, the service provider can ask for these address ranges at provisioning. (Network Operators may not be able to comply with this practice on links to upstream/downstream providers or peering links, since the

valid source address space is not known).

- ID Network Reliability Functions: Network Operators, Service Providers, Equipment Suppliers and Property Managers should assess the functions of their organization and identify those critical to ensure network reliability.
- BGP Authentication: Network Operators and Service Providers should authenticate BGP sessions (e.g., using TCP MD5) with their own customers and other providers.
- Network Operators, Service Providers and Equipment Suppliers should, where programs exist, coordinate with local, state and/or federal emergency management and law enforcement agencies for pre-credentialing to help facilitate access by technicians to restricted areas during an event.
- Network Operators should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with site-specific constraints, criticality of the site, the expected load and reliability of primary power.
- Network Operators and Property Managers should consider placing fixed power generators at cell sites, where feasible.
- Network Operators and Property Managers should consider pre-arranging contact information and access to restoral information with local power companies.
- Network Operators and Service Providers should consider ensuring that the back-haul facility equipment located at the cell site is provided with backup power duration that is equal to that provided for the other equipment at the cell site.
- Service Providers should establish agreements with Property Managers for both regular and emergency power.
- Network Operators, Service Providers and Property Managers should consider providing diversity within power supply and distribution systems so that single point failures (SPOF) are not catastrophic. For large battery plants in critical offices, consider providing dual AC feeds (odd/even power service cabinets for rectifiers). Transfer switches should be listed to a UL standard for Transfer Switch Equipment. When transfer breaker systems are used, they must be mechanically and electrically interlocked.
- In order to prepare for contingencies, Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire departments and other security and emergency agencies to exchange critical information related to threats, warnings and mutual concerns.

As you can see, CSRIC provides a deeply detailed set of standards and best practices for communications providers and ISPs to deploy. Following these recommendations will place your business in an excellent position to protect both data and infrastructure.

Security Operational Third-Party Audits and Certifications

If your company is comfortable with the depth of its technical and physical data security architecture and its operational policy structure, then you may want to consider bringing in a high-level consulting firm to certify your company's security practices. Be forewarned that such certification does not come cheap. Even if your systems are entirely up to speed and your company will not need remediation to be certified, the exercise will most certainly cost $50,000 to $100,000 or more. If your systems are not fully ready and documented so they can be certified, expect to spend a multiple of those numbers.

The advantage to most of the best-known certifications is that the credential demonstrates a commitment to operational competence in security, and a (refutable) argument that your company has met its industry standards. This could be important to tout following a significant data exposure incident, a regulatory investigation or a consumer lawsuit. These certifications are additional sets of credentials that can be recognized by regulators and juries. If your company accepts payment cards, then the payment card industry third-party audit is unavoidable, but the other standard audits sold by the accounting and consulting industries may or may not help your company.

Receiving a consulting/accounting firm's certification is not a panacea. Some of the certifications like a Statement on Auditing Standards (SAS) No. 70 Type I audit do little more than validate that your company has a written operational security plan, without even checking if your company is implementing the plan. The different types of certification audits vary in measuring criteria, expense and usefulness, but they are generally inappropriate for small companies and most larger companies can purchase similar benefits without the time and expense that these audits entail. The rest of this section discusses the best known third-party operational security audit standards and their areas of utility for the communications industry.

SAS 70 reports have been around a very long time and suffer from being a relatively unsophisticated and not very useful way of measuring a company's cybersecurity. The report originated with the American Institute of Certified Public Accountants and only a licensed CPA can provide your company with a SAS 70 certification. Needless to say, in the past 25 years, professionals have learned that many people other than CPAs are better-educated and more trustworthy in evaluating network security.

The SAS 70 service auditor's report contains the auditor's opinion, a description of the controls placed in operation, and, if the report is SAS Type II, a description of the auditor's tests of operating effectiveness. In this scheme, the subject company chooses what it will be audited on. This certification cannot be used to demonstrate compliance with legal security requirements like the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or even the Payment Card Industry Data Security Standard (PCI DSS).

SAS 70 is not a predetermined set of standards that an organization must meet to be certified. SAS 70 is a mechanism to document a control environment and its operation, and is not a

standard for the operation of a secure environment. Most security professionals will tell you that if SAS 70 was ever relevant, that time has passed, although Google Apps and Rackspace are both SAS 70 certified, so some institutions are finding value in it. This is the certification audit you try to secure when your company has documented security policies but not deep technology investments in security.

SAS 70 has been largely phased out and even surpassed among the accountants by SSAE (the Statement on Standards for Attestation Engagements) 16, which reports on the use and treatment of financial information. SSAE 16 exceeds SAS 70 by not only verifying the company's controls and processes, but also requiring a written assertion regarding the design and operating effectiveness of the controls being reviewed. This audit results in a Service Organization Control (SOC) 1 report, focused on internal financial controls. A SOC 1, Type 1 report focuses on the auditors' opinion of the accuracy and completeness of the data center management's design of controls, system and/or service. A SOC 1, Type 2 report includes Type 1 and an audit on the effectiveness of controls over a certain time period, normally between six months and a year. SOC 2 and SOC 3 provide pre-defined, standard benchmarks for controls related to the security, availability, processing integrity, confidentiality, or privacy of a system and its information. Once again, this standard audit can only be provided by CPAs, and many executives see it as a way to generate audit work and keep accountants relevant in the age of information technology. It tends to be used by the financial services industry to demonstrate compliance that would be relevant under the Gramm-Leach-Bliley Act (GLBA).

The International Organization for Standardization (ISO), a non-governmental standard setting body comprising representatives of many nations' national standards organizations, and the International Electrotechnical Commission (IEC), an independent standards body in the electrical, electronic and related technology areas, have issued a relevant set of standards as the ISO/IEC 27000 series for information security controls. This family of standards provides best practice recommendations for information security management. (You may be familiar with the ISO 9000 series of best practice recommendations for quality assurance). The security management standards are broadly written and are meant to be applicable to companies of all sizes and in all sectors. The standards change as technology changes.

The core of the ISO 27000 series and the most globally accepted set of general information security standards is ISO/IEC 27001:2013 (also known as ISO 27001), which sets out the requirements against which an organization's information security management system (ISMS) can be audited and certified. All the other standards in the ISO 27000 family support the ISO 27001 standard. Some organizations choose to implement the standard in order to benefit from the best practice it contains while others decide they also want to get certified to reassure customers and clients that its recommendations have been followed. ISO does not perform certification, but technology auditors can evaluate your company's systems under these standards. Once obtained, the ISO

27001 certification lasts 3 years. ISO 27001 shares many similarities with HIPAA and PCI DSS requirements, but cannot be substituted for required compliance to these standards. ISO 27002 is the set of best practices that tells a company how to become compliant with ISO 27001. Amazon Web Services and Microsoft Office 365 are both ISO 27001 certified. Security professionals generally believe that ISO 27001 is the best general purpose form of information security attestation available right now.

Other public and private information security audit standards exist and are requested by contracting parties to establish that a company is performing objective best practices, and third-party consultants can be enlisted to certify your organization under these standards. However, for a data security audit that is not mandated by the government, the ISO 27001 is the one most accepted and highly likely to demonstrate a strong organizational data security program and practices.

PCI DSS — Requirements for Accepting Credit Cards as Payment

Most communications businesses accept credit cards as payment for services, and if your company allows credit or debit card payment, then it is subject to the Payment Card Industry Data Security Standards (PCI DSS). These standards are contractually required of retailers that wish to participate in the payment card ecosystem. The PCI standards are enforced not directly by the card companies, but by the merchant banks who enforce them against their client retailers. Card processors are also involved in the system, so that fines under the PCI DSS may be withdrawn from the credit and debit card payment systems before they reach your business's account.

The goal of the PCI DSS is to protect cardholder data and sensitive authentication data wherever it is processed, stored or transmitted. The security controls and processes required by PCI DSS propose to protect all payment card account data. One important rule is that merchants, service providers, and other entities involved with payment card processing must never store sensitive authentication data after authorization. This includes the 3- or 4- digit security code printed on the front or back of a card, the data stored on a card's magnetic stripe or chip (also called "Full Track Data"), and personal identification numbers (PIN) entered by the cardholder.

A payment card council is responsible for managing the data security standards, but each payment card brand maintains its own separate compliance enforcement programs. Each payment card brand has defined specific requirements for compliance validation and reporting, such as provisions for performing self-assessments. Depending on an entity's classification or risk level (determined by the individual payment card brands), processes for compliance usually follow these steps:

1. **Scope:** determine which system components and networks are in scope for PCI DSS
2. **Assess:** examine the compliance of system components in scope following the testing procedures for each PCI DSS requirement

3. **Report:** assessor and/or entity completes required documentation (e.g. Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC), including documentation of all compensating controls
4. **Attest:** complete the appropriate Attestation of Compliance (AOC)
5. **Submit:** submit the form SAQ, ROC, AOC and other requested supporting documentation such as ASV scan reports to the acquirer (for merchants) or to the payment brand/requestor (for service providers)
6. **Remediate:** if required, perform remediation to address requirements that are not in place, and provide an updated report

Both PCI DSS and the payment card brands strongly discourage storage of cardholder data by merchants and processors. There is no need, nor is it allowed, to store data from the magnetic stripe on the back of a payment card. If merchants or processors have a business reason to store front-card information, such as name and account number, PCI DSS requires this data to be encrypted or made otherwise unreadable. The best practice in this case may be to outsource the entire processing of cards to an expert in the subject. The best way to avoid exposing or losing card information is to never hold that information. If your company chooses to take the outsourcing route, take a careful look at the vendor's agreement, and make certain that your processor promises to be PCI DSS compliant.

The PCI DSS specifically provides that a service provider or merchant may use a third-party service to store, process, or transmit cardholder data on their behalf, or to manage CDE components. Parties should clearly identify the services and system components that are included in the scope of the service provider's annual onsite PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements which are the responsibility of the service provider's customers to include in their own PCI DSS reviews. If the third party undergoes its own PCI DSS assessment, it should provide sufficient evidence to its customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. The service provider Attestation of Compliance includes a table that summarizes PCI DSS requirements covered and the specific service(s) assessed, and can be provided to customers as evidence of the scope of a service provider's PCI DSS assessment. However, the specific type of evidence provided by the service provider to its customers will depend on the agreements/contracts in place between those parties. Companies must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data.

Part of your required actions under the PCI DSS is finding a third party who will assess your company's compliance with the standards. The PCI Council manages programs that will help facilitate the assessment of compliance with PCI DSS: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs are approved by the PCI Council to assess compliance with the PCI DSS. ASVs are approved by the PCI Council to validate adherence to the PCI DSS scan requirements by performing vulnerability scans of internet-facing environments of merchants and service providers. The PCI Council

also provides PCI DSS training for Internal Security Assessors (ISAs). Using a PCI Council approved consultant to assess your business is a best practice. They sometimes charge more than other assessors, but their findings are more readily accepted by the banks and card companies.

The 12 Requirements of the PCI DSS

Understanding and implementing the 12 requirements of PCI DSS can seem daunting, especially for companies without a substantial security budget or a large IT department. However, PCI DSS mostly calls for good, basic security. Even if there was no requirement for PCI compliance, the best practices for security contained in the standard are steps that every business would want to take anyway to protect sensitive data and continuity of operations.

Here are the 12 requirements and the published sub requirements beneath them:

1. **Install and maintain a firewall configuration to protect cardholder data**
   - 1.1. Establish and implement firewall and router configuration standards that formalize testing whenever configurations change; that identify all connections between the cardholder data environment and other networks (including wireless) with documentation and diagrams; that document business justification and various technical settings for each implementation; that diagram all cardholder data flows across systems and networks; and that stipulate a review of configuration rule sets at least every six months.
   - 1.2. Build firewall and router configurations that restrict all traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment.
   - 1.3. Prohibit direct public access between the internet and any system component in the cardholder data environment.
   - 1.4. Install personal firewall software or equivalent functionality on any devices (including company and/or employee owned) that connect to the internet when outside the network (for example, laptops used by employees), and which are also used to access the cardholder data environment.
   - 1.5. Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

2. **Do not use vendor-supplied defaults for system passwords and other security parameters**
   - 2.1. Always change ALL vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.

2.2. Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified.

2.3. Using strong cryptography, encrypt all non-console administrative access. (Where Secure Sockets Layer (SSL)/early Transport Layer Security (TLS) is used, the requirements in PCI DSS Appendix A2 must be completed.)

2.4. Maintain an inventory of system components that are in scope for PCI DSS.

2.5. Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

2.6. Shared hosting providers must protect each entity's hosted environment and cardholder data (details are in PCI DSS Appendix A1: "Additional PCI DSS Requirements for Shared Hosting Providers.")

Protect Cardholder Data

3. Protect stored cardholder data

3.1. Limit cardholder data storage and retention time to that which is required for business, legal, and/ or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.

3.2. Do not store sensitive authentication data after authorization (even if it is encrypted). Render all sensitive authentication data unrecoverable upon completion of the authorization process. Issuers and related entities may store sensitive authentication data if there is a business justification, and the data is stored securely.

3.3. Mask PAN when displayed (the first six and last four digits are the maximum number of digits you may display), so that only authorized people with a legitimate business need can see more than the first six/last four digits of the PAN. This does not supersede stricter requirements that may be in place for displays of cardholder data, such as on a point-of-sale receipt.

3.4. Render PAN unreadable anywhere it is stored — including on portable digital media, backup media, in logs, and data received from or stored by wireless networks. Technology solutions for this requirement may include strong one-way hash functions of the entire PAN, truncation, index tokens with securely stored pads, or strong cryptography. (See PCI DSS Glossary for definition of strong cryptography.)

3.5. Document and implement procedures to protect any keys used for encryption of cardholder data from disclosure and misuse.

3.6. Fully document and implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.

3.7. 3.7 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

4. **Encrypt transmission of cardholder data across open, public networks**
   - 4.1. Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices to implement strong encryption for authentication and transmission. (Where SSL/early TLS is used, the requirements in PCI DSS Appendix A2 must be completed.)
   - 4.2. Never send unprotected PANs by end user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
   - 4.3. Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Maintain a Vulnerability Management Program

5. **Protect all systems against malware and regularly update antivirus software or programs**
   - 5.1. Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). For systems not affected commonly by malicious software, perform periodic evaluations to evaluate evolving malware threats and confirm whether such systems continue to not require anti-virus software.
   - 5.2. Ensure that all anti-virus mechanisms are kept current, perform periodic scans, and generate audit logs, which are retained per PCI DSS Requirement 10.7.
   - 5.3. Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.
   - 5.4. Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.
6. **Develop and maintain secure systems and applications**
   - 6.1. Establish a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. “high,” “medium,” or “low”) to newly discovered security vulnerabilities.
   - 6.2. Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
   - 6.3. Develop internal and external software applications including web-based administrative access to applications in accordance with PCI DSS and based on industry best practices. Incorporate information security throughout the software development life cycle. This applies to all software developed internally as well as bespoke or custom software developed by a third party. Create policy governing security

controls according to industry standard best practices. Regularly scan systems for vulnerabilities. Create remediation schedule based on risk and priority. Pre-test and deploy patches. Rescan to verify compliance. Update security software with the most current signatures and technology. Use only software or systems that were securely developed by industry standard best practices.

6.4. Follow change control processes and procedures for all changes to system components. Ensure all 18 relevant PCI DSS requirements are implemented on new or changed systems and networks after significant changes.

6.5. Prevent common coding vulnerabilities in software development processes by training developers in secure coding techniques and developing applications based on secure coding guidelines, including how sensitive data is handled in memory.

6.6. Ensure all public-facing web applications are protected against known attacks, either by performing an application vulnerability assessment at least annually and after any changes, or by installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

6.7. Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know

7.1. Limit access to system components and cardholder data to only those individuals whose job requires such access. Restrict Access to Cardholder Data Environments by employing access controls. Limit access to only those individuals whose job requires such access. Formalize an access control policy that includes a list of who gets access to specified cardholder data and systems. Deny all access to anyone who is not specifically allowed to access cardholder data and systems.

7.2. Establish an access control system(s) for system components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.

7.3. Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

8. Identify and authenticate access to system components

8.1. Define and implement policies and procedures to ensure proper user identification management for users and administrators on all system components. Assign all users a unique username before allowing them to access system components or cardholder data.

8.2. Employ at least one of the following methods to authenticate all users: something you know, such as a password or passphrase; something

you have, such as a token device or smart card; or something you are, such as a biometric. Use strong authentication methods and render all passwords/passphrases unreadable during transmission and storage using strong cryptography.

8.3. Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication. This requires that at least two of the three authentication methods described in 8.2 are used for authentication. Using one factor twice (e.g. using two separate passwords) is not considered multi-factor authentication. This requirement applies to administrative personnel with non-console access to the CDE from within the entity's network, and all remote network access (including for users, administrators, and third parties) originating from outside the entity's network. (Note: The requirement for multi-factor authentication for non-console administrative access from within the entity's network was a best practice until January 31, 2018, after which it became a requirement.) IDENTIFY AND AUTHENTICATE ALL USERS. Every user with access to the Cardholder Data Environment must have a unique ID. This allows a business to trace every action to a specific individual. Every user should have a strong password for authentication.

8.4. Develop, implement, and communicate authentication policies and procedures to all users.

8.5. Do not use group, shared, or generic IDs, or other authentication methods. Service providers with access to customer environments must use a unique authentication credential (such as a password/passphrase) for each customer environment.

8.6. Use of other authentication mechanisms such as physical security tokens, smart cards, and certificates must be assigned to an individual account.

8.7. All access to any database containing cardholder data must be restricted: all user access must be through programmatic methods; only database administrators can have direct or query access; and application IDs for database applications can only be used by the applications (and not by users or non-application processes).

8.8. Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

9. Restrict physical access to cardholder data

9.1. Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

9.2. Develop procedures to easily distinguish between onsite personnel and visitors, such as assigning ID badges.

9.3. Control physical access for onsite personnel to the sensitive areas. Access must be authorized and based

on individual job function; access must be revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc. returned or disabled. Businesses must physically secure or restrict access to printouts of cardholder data, to media where it is stored, and devices used for accessing or storing cardholder data. It's important to understand that PCI is about protecting both electronic data and paper receipts as well.

9.4. Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained, given a physical badge or other identification that expires and identifies visitors as not onsite personnel, and asked to surrender the physical badge before leaving the facility or at the date of expiration. Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name, company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law.

9.5. Physically secure all media; store media back-ups in a secure location, preferably off site.

9.6. Maintain strict control over the internal or external distribution of any kind of media.

9.7. Maintain strict control over the storage and accessibility of media.

9.8. Destroy media when it is no longer needed for business or legal reasons.

9.9. Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. This includes periodic inspections of POS device surfaces to detect tampering, and training personnel to be aware of suspicious activity.

9.10. Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

10.1. Implement audit trails to link all access to system components to each individual user.

10.2. Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; and creation and deletion of system-level objects.

10.3. Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication,

origination of event, and identity or name of affected data, system component or resource.

10.4. Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time.

10.5. Secure audit trails so they cannot be altered.

10.6. Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.

10.7. Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.

10.8. Service providers must implement a process for timely detection and reporting of failures of critical security control systems.

10.9. Ensure related security policies and operational procedures are documented, in use, and known to all affected parties.

11. Regularly test security systems and processes

11.1. Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Maintain an inventory of authorized wireless access points and implement incident response procedures in the event unauthorized wireless access points are detected.

11.2. Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Address vulnerabilities and perform rescans as needed, until passing scans are achieved. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, complete four consecutive quarters of passing scans. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes and internal scans may be performed by internal staff.

11.3. Develop and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or modification. If segmentation is used to reduce PCI DSS scope, perform penetration tests at least annually to verify the segmentation methods are operational and effective. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after making changes to these controls.

11.4. Use network intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures

must be kept up to date. To demonstrate compliance, internal scans must not contain high-risk vulnerabilities in any component in the cardholder data environment. For external scans, none of those components may contain any vulnerability that has been assigned a Common Vulnerability Scoring System (CVSS) base score equal to or higher than 4.0.

11.5. Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert 24 personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly. Implement a process to respond to any alerts generated by the change-detection solution.

11.6. Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all

12.1. Establish, publish, maintain, and disseminate a security policy; review the security policy at least annually and update when the environment changes.

12.2. Implement a risk assessment process that is performed at least annually, and upon significant changes to the environment, that identifies critical assets, threats, and vulnerabilities, and results in a formal assessment.

12.3. Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and internet.

12.4. Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. Service providers must also establish responsibility for their executive management for the protection of cardholder data and a PCI DSS compliance program.

12.5. Assign to an individual or team information security responsibilities defined by 12.5 subsections.

12.6. Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

12.7. Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. Example screening includes previous employment history, criminal record, credit history, and reference checks.

12.8. Maintain and implement policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.

12.9. Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data that they possess or otherwise store, process, or transmit on behalf of the customer, or to the

extent they could impact the security of the customer's cardholder data environment.

12.10. Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.11. Service providers must perform and document reviews at least quarterly to confirm personnel are following security policies and operational procedures.

PCI DSS compliance should not be seen in isolation, but as part of a comprehensive information security and risk-management strategy. A PCI DSS assessment can uncover important security gaps that should be fixed, but it is no guarantee that customer's data and your company reputation are safe.

Requirements: Compensating controls may be considered for most PCI DSS requirements when a company cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of compensating controls. In order for a compensating control to be considered valid, it must be reviewed by an assessor. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Entities should be aware that a particular compensating control will not be effective in all environments. See PCI DSS Appendices B and C for details.

National Institute of Standards in Technology (NIST) Telecommunications Security Guidelines

NIST, the federal government agency charged with creating technical standards for industry and government including official weights and measures, has developed two primary documents of interest for the telecommunications industry. First is the NIST Framework for Improving Critical Infrastructure Cybersecurity. And second, the NIST Telecommunication Security Guidelines for Telecommunication Managed Networks (TMNs), specifically applies to this industry. Both can be important guides for strong security practices and demonstrating that your security architecture was developed around these frameworks will impress your regulators, who reference these standards regularly.

NIST frameworks are technology neutral and are meant to be applied in the most logical manner for your organization's particular needs. As NIST states in the Critical Infrastructure Framework, "Organizations will continue to have unique risks — different threats, different vulnerabilities, different risk tolerances — and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better

managing cybersecurity risks." This Framework is expected to be regularly updated and improved with industry feedback.

The Critical Infrastructure Framework is built around five core functional elements intended to be performed concurrently and continuously to address dynamic cyber risks: Identify, Protect, Detect, Respond, and Recover. Companies should study these functions and build security regimes around each concept. NIST breaks down the functions into individual categories containing more specific actions for an organization to take.

For detailed information about the NIST Framework and its use, please review the **NTCA Cybersecurity Series Part 3: Sector** Specific Guide to the NIST Cybersecurity Framework. The Guide was developed to help your operational staff evaluate your company's cybersecurity program at a more granular and sophisticated level.

NIST Advice on Securing SCADA Networks

Supervisory control and data acquisition (SCADA) networks include computers and applications that perform key functions in telecommunications businesses, but they also present a security risk. SCADA networks were initially designed to maximize functionality, with little attention paid to security. As a result, performance, reliability, flexibility and safety of distributed control/SCADA systems are robust, while the security of these systems is often weak. This makes some SCADA networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions. For these reasons, NIST issued a paper on 21 steps to improve cybersecurity of SCADA networks.
The recommended steps are:

1. Identify all connections to SCADA networks.
2. Disconnect unnecessary connections to the SCADA network.
3. Evaluate and strengthen the security of any remaining connections to the SCADA network.
4. Harden SCADA networks by removing or disabling unnecessary services.
5. Do not rely on proprietary protocols to protect your system.
6. Implement the security features provided by device and system vendors.
7. Establish strong controls over any medium that is used as a backdoor into the SCADA network.
8. Implement internal and external intrusion detection systems and establish 24/7 incident monitoring.
9. Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.
10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.
11. Establish SCADA "Red Teams" to identify and evaluate possible attack scenarios.

12. Clearly define cybersecurity roles, responsibilities, and authorities for managers, system administrators, and users.
13. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.
14. Establish a rigorous, ongoing risk management process.
15. Establish a network protection strategy based on the principle of defense-in-depth.
16. Clearly identify cybersecurity requirements.
17. Establish effective configuration management processes.
18. Conduct routine self-assessments.
19. Establish system backups and disaster recovery plans.
20. Senior organizational leadership should establish expectations for cybersecurity performance and hold individuals accountable for their performance.
21. Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

The NIST document contains detailed explanations for each of these recommendations.

Any or all of these standards are respected by the telecommunications regulators and the PCI DSS are required for companies accepting card payments. While no one standard will ever be dispositive for all size companies with varying resources – especially given the pace of change in technology and threats – all telecommunications companies can pull valuable lessons from each of these relevant standards.

Resources

- The PCI Standards can all be downloaded from the PCI Document Library
- PCI Security Standards Council Web site: **www.pcisecuritystandards.org**
- **PCI DSS FAQ**
- **PCI DSS Approved PIN Security Devices**
- **PCI Approved Payment Applications**
- **PCI P2PE Solutions**
- **PCI Approved Assessors**
- **PCI Approved Vendors**
- **PCI DSS The Standard**
- **PCI DSS Supporting Documents**
- **PCI DSS Self-Assessment**
- **PCI DSS Glossary Bell Labs Best Practices Main Page**
- **Physical Security Best Practices**
- **Cybersecurity Best Practices**

- **NTCA's Cybersecurity Series *Part 3: Sector-Specific Guide to NIST Cybersecurity Framework***
- **US-CERT web site.**
- **US-CERT tips web site.**
- **NIST SCADA Security Advice**
- **NIST Cybersecurity Framework**
- **NIST Telecommunications Security Guidelines for TMN**

CREATING THE WRITTEN INCIDENT RESPONSE PLAN

Introduction

A data security "incident" refers to any unauthorized access to confidential data, or any exploitation of or attack against a website, network, or other information technology system. Typically, this includes any kind of "data breach," ranging from a laptop accidentally left on a park bench, to theft of valuable personal information or trade secrets by computer hackers on the other side of the planet. But it could also include a variety of other cybercrime – such as ransomware that encrypts an organization's critical data and captures important data for extortion, or distributed denial of service (DDoS) that overruns a website with traffic causing it to stop working.

Whatever the data security incident that may have occurred, "incident response" refers to what the organization does to detect, address, and recover from what happened. Broadly speaking, the process of incident response should include at least these steps, which often overlap:

1. Detect and verify that a data security incident has occurred.
2. Contain and mitigate any ongoing data breach or system compromise.
3. Investigate what occurred and what data or systems were affected.
4. Analyze legal obligations triggered by the incident, as well as business or liability risk.
5. Notify individuals affected, law enforcement, and any others as necessary.
6. Review applicable cybersecurity controls or other safeguards, and make appropriate improvements based on lessons learned from the incident.

Properly carrying out an incident response is easier said than done. Indeed, it can be very challenging during the intense pressure created by a major data breach or cyberattack. That is why it is crucial to maintain a written incident response plan (WIRP) to be followed in case of a data security incident. For some organizations, this could even be required by law as part of risk management. This section of the guide provides instruction on how to create and maintain a WIRP, including the key elements, best practices to make it effective, and examples of sample language and strategy to implement a response plan. WIRP's are not "one size fits all," and this guide cannot replace an actual WIRP that is tailored to your organization's unique set of needs. Use the information in this guide to work with your attorneys and your technical consultants to develop your WIRP.

Prior to Drafting: How to Prepare for the WIRP

Inventory Your Data Management and Information Technology Systems

In order to prepare a thorough and effective WIRP, you should first try to determine what types of data your organization stores, where that data rests or moves within your network, what cybersecurity controls or other safeguards are in place, and the overall architecture of your computer network and

information technology (IT) systems. You should also try to identify any third parties who have access to your data or systems, or who provide cloud-hosting service or other processing for data controlled by your organization. In the event of a data security incident, you will want to have already explored these questions to make it possible to determine which data or systems may have been compromised, the potential harm to affected individuals, and what legal obligations may be triggered by the incident. They also inform which people and systems will need to be involved in the incident response. Notably, this type of inventory assessment could involve working with an outside information security firm with the necessary technical expertise. The "Asset Management" and "Risk Assessment" sections of the NIST Cybersecurity Framework encompass this type of inventory. See Attachment A.

Identify Your Breach Notification Obligations

Identifying what, if any, legal obligations your organization may have to notify others following a data breach or other data security incident is critical. These will include obligations to notify affected individuals or regulators pursuant to state breach notification statutes, and perhaps obligations related to credit card data under the Payment Card Institute Data Security Standard (PCI DSS) if your organization accepts credit card payments. Moreover, the FCC has imposed regulations requiring telecommunications carriers to notify law enforcement about a breach of the customer proprietary network information (CPNI) of their subscribers. However, depending on what types of data your organization holds and the circumstances of your business, there may well be other statutory or regulatory obligations to notify others following a data breach. You may also have contractual obligations to notify third-party businesses about a data security incident, and conversely, they may have similar obligations to you. Similar to the mapping of data and network architecture, it may be advisable to perform this type of legal assessment in consultation with an outside law firm that has the necessary experience in privacy and data security law to identify your contractual obligations.

Assemble the Incident Response Team

A central feature of the WIRP is to designate the team of people ("IR Team") who will be responsible for managing your organization's incident response and implementing the incident response plan. At minimum, this team should include representatives from the following functions within your organization:

Information technology and security	Being most familiar with information technology systems and the cybersecurity controls in place, works to mitigate, investigate, and remediate the data security incident, usually assisting an outside data security forensics firm.
Legal and compliance	Identifies and ensures compliance with legal obligations such as breach notification, handles internal investigation, ensures that

	communications and records are protected by privilege, and assists post-incident assessment of lessons learned – utilizing advice of outside legal counsel specializing in privacy and data security law.
Executive management	Provides and exercises the authority needed to execute the WIRP quickly during a crisis.
Communications	Handles internal communications about the incident and manages external communications, often through an outside public relations firm that specializes in crisis management.
Human resources	Addresses issues regarding the breach of sensitive employee data or regarding employee conduct relevant to the internal investigation.
Customer service	Fields questions and addresses concerns from customers, rebuilds customer trust, and helps individuals affected by a data breach try to minimize their risk of identity theft.

Determine the Scope and Application

Finally, you need to decide what types of situations the WIRP will address, what types of data require a breach response protocol, and under what circumstances will a data security incident be escalated to the IR Team. For instance, an employee forgetting his laptop at the airport would probably be approached differently than a ransomware attack shutting down business operations. Likewise, you will need to decide whether the WIRP should apply to all parts of the organization, and also how to coordinate with affiliates or third parties who may fall within the scope of incident response.

Pen to Paper: Drafting the WIRP

Purpose and Scope

Begin by explaining the objective and reason for the WIRP, referencing compliance with a relevant legal requirement as appropriate. Regarding scope, the WIRP should make clear to whom the policy applies and how it interacts with other company policies related to privacy and

information security. The WIRP must also define "data security incident," "personal information," and similar terms which are referenced in the WIRP and trigger its operation.

Sample Language

"Data security incident" includes any actual or reasonably suspected loss or theft of, or unauthorized disclosure, acquisition, access or use of, the organization's websites, systems, networks, data, computers and other devices and information technology ("IT") systems, including data held or IT services provided by third-party service providers, that results in compromised integrity, confidentiality and/or availability of such systems, devices, or information.

IR Team Membership and Contact Information

Identify the members of the IR Team by name, title, department and contact information—and make sure this information is kept up to date. The contact information of the IR Team should include multiple channels of communication, such as email, phone number (cell and office) and alternative contact channels in the event that the office communications are disrupted. If you have a relatively small IR Team (one to two individuals), designate a back-up person to accept reports in the event that IR Team members are unavailable. You may also consider creating a generic email address for incident response that is regularly checked by an IR Team member and can be used to receive reports and answer questions.

IR Team Responsibilities

The WIRP should explain the IR Team's role and responsibility to execute a prompt and effective response to data security incidents according to the terms of the WIRP, and expressly authorize the IR Team to take the steps which are necessary to carry out that responsibility. The WIRP should also describe specific responsibilities for the IR Team, as appropriate.

Sample Language

The IR Team must do the following:

- Monitor for data security incidents;
- Promptly and effectively respond to any data security incidents;
- Contact legal counsel to discuss the incident and determine whether the incident rises to the level of a data breach;
- Investigate data security incidents, including preliminary and formal investigations;
- Report findings to management and appropriate authorities;
- Manage internal and external communications regarding any data security incidents;
- After resolving a data security incident, review and assess the response;
- Create a database to track all reported data security incidents;
- Create a risk rating to classify incidents as low, medium, or high risk; and
- Review and update contact information for IR Team members and communicate this information to everyone to whom the WIRP applies.

Reporting Processes and Obligations

The WIRP should identify processes available for detecting data security incidents, such as self-reporting by employees, automated detection means, and third-party reports. It should also establish an appropriate infrastructure for the reporting of suspected data security incidents. One or more designated IR Team members should be responsible for maintaining up-to-date contact information for the reporting of incidents and for ensuring that this information is adequately communicated to employees and contractors who may need to report an incident, including third-party vendors.

The WIRP should set forth clear reporting obligations in the event of a data security incident, making clear that employees and contractors are required to report data security incidents immediately when they become aware of such an incident. Employees reporting a data security incident should also notify their supervisor, who should separately alert the IR Team.

Sample Language

1) The Company shall develop, implement, and periodically update procedures to detect and assess potential data security incidents, including through automated detection means and through reports from internal and external sources.

2) Employees or others with authorized to access the Company's IT systems, network, or data shall immediately report any actual or suspected data security incident to [IR Team contact].

3) Third parties who claim to have information regarding an actual or alleged data security incident should be directed to [IR Team contact], and employees who receive external communications regarding a potential data security incident or cybersecurity vulnerability affecting the Company shall immediately report such communications.

In addition, the WIRP should make one or more IR Team members responsible for monitoring for data security incidents, creating a database to track all reported incidents, and creating a risk rating which classifies reported incidents as low, medium, or high to facilitate the appropriate escalation and response.

Initial Verification and Assessment

If a potential data security incident is reported, then the IR Team should immediately begin a preliminary investigation to determine whether a data security incident has in fact occurred and to assess its nature and severity. The scope of such investigation may depend on the particular circumstances, but for any data security incident the IR Team should look for what caused the incident, determine if it remains ongoing, and assess whether it carries a low, medium, high, or unknown risk level. The WIRP should make clear that the risk level should be re-assessed continuously as more facts and evidence come to light.

In making the assessment of risk level, the following are basic factors for the IR Team to take into account under the WIRP:

1. Type of incident (e.g., extortion, stolen data, or lost device),
2. Nature of the data that may be affected,
3. Intent behind the incident (e.g., criminal conduct or honest mistake),
4. Scope of incident (e.g., entire database or single employee file), and
5. Impact on current business functions (e.g., system outage or public outcry)

In this analysis, the type of data affected and related circumstances may be particularly important. On one hand, the incident might involve highly confidential information, sensitive employee or customer personal information, or encrypted confidential data along with the access key — which would usually carry a higher risk level. On the other hand, the incident might

involve information in aggregate form, encrypted data without the necessary access key, or non-personal information — which would usually carry a lower risk level.

Fully Investigate and Develop a Response

The WIRP should set forth the procedure for a formal investigation of the data security incident. Most small businesses do not have the internal resources or expertise to fully investigate a major data security incident and should retain a data security forensics firm and outside legal counsel specializing in privacy and cybersecurity law. Based upon what is learned through this full investigation of the data security incident, the WIRP should then provide for the IR Team to decide upon and implement a plan of action to respond.

Sample Language

Following verification and initial assessment of a data security incident, the IR Team shall thoroughly investigate the data security incident, analyse the nature and extent of potential harm to the Company and to affected individuals, and formulate an appropriate response plan to contain, remediate, and recover from the incident. The IR Team shall also document its investigation and analysis regarding each data security incident.

Accordingly, under the WIRP, the overall investigation should have the following goals:

1. Identify if the data security incident remains ongoing;
2. Stop the incident and mitigate any damage;
3. Collect thorough facts about the incident (such as through interviews, cybersecurity forensic analysis, and other methods);
4. Create a timeline of the incident;
5. Attempt to identify the attacker, if appropriate;
6. Document the investigation;
7. Detect any vulnerabilities exploited;
8. Recommend steps to address the underlying cause of the incident; and
9. Enable your legal department or outside counsel to identify legal obligations

Identify Notification Obligations

The WIRP should designate an individual responsible for working with the legal team to identify the legal obligations and liability risk which may arise out of a data security incident. For

example, if the initial assessment indicates that personal information may be affected (such as an individual's name plus his driver's license number, Social Security number, payment card information, email address plus password, or other non-public information identifying an individual), then the WIRP should require the IR Team to coordinate with internal or outside counsel to determine what reporting obligations may be trigged by a data breach. Certain breach notification statutes require notice to regulators within 48 hours, making it critical that incidents are reported promptly and investigated once reported.

Sample Language

The IR Team shall coordinate with legal counsel to identify and comply with all laws, regulations, and contractual obligations that require notifying other parties about the data security incident. Wherever required, and in consultation with legal counsel, the IR Team shall notify law enforcement, individuals whose personal information was affected, applicable regulators or other authorities, business associates according to agreements, the relevant insurance carrier, and any other parties affected. The IR Team may also make or authorize further discretionary communications about a data security incident where appropriate.

Preservation and Collection of Evidence

The WIRP should take into account best practices on preserving and collecting evidence. For example, the IR Team may have to decide whether to immediately deactivate a system to prevent additional unauthorized activity or to allow it to continue for a short period of time so that law enforcement or investigators can further analyze the incident. Members of the IR Team and others involved in the investigation and data security incident should limit information sharing to those with a need-to-know basis, especially early in the investigation process. The IR Team should provide clear and consistent reporting and notifications. At all steps in the process, emphasis should be placed on maintenance of records on the data security incident and how the organization responded to the incident. The WIRP should encourage investigation and reporting that is done in a manner that protects the legal privileges available (such as, attorney-client privileges, attorney work-product doctrine, etc.).

Identify External Resources

Identify the external resources that may be required in the WIRP. The key external resources should be pre-screened and made aware that they will form part of the IR Team if requested. For example, consider including name and contact information for: (1) vendor or service provider representatives; (2) outside legal counsel; (3) your cybersecurity insurance provider; (4)

cyber forensics investigators or other technical experts; (5) crisis communication specialists; and (6) breach notification and identity theft prevention and mitigation service providers.

In determining whether to use internal or external resources, consider whether your organization has the specialized skills necessary to provide the service (e.g., to locate or preserve applicable evidence or to comply with state breach reporting obligations) and whether there are any potential conflicts of interest with having an internal employee carry out the response function. Note, for example, that certain self-regulation regimes, such as PCI DSS, may view third-party forensics investigators as having specialized expertise and greater freedom to carry out an investigation.

Working with Law Enforcement

The WIRP should identify and designate an individual from the IR Team or legal counsel to be responsible for having primary contact with law enforcement, including federal investigatory agencies and local law enforcement.

Generally speaking, companies are encouraged to notify federal law enforcement about any data security incident that:

1. Involves a significant loss of data or system integrity;
2. Impacts a large number of individuals; Involves unauthorized access to or malware found on critical IT systems;
3. Affects critical infrastructure or core government functions; or
4. Impacts national security, economic security, or public health and safety.

FCC regulations and some States mandate that companies report data security incidents to law enforcement, depending on the circumstances. Conversely, legal obligations to make breach notification to affected individuals can often be delayed when requested by law enforcement so as not to interfere with a confidential investigation. The Treasury Department encourages reporting of ransomware attacks to law enforcement, even if the victim intends to pay the ransom requested by the criminal.

Reports of cybercrime may be made through local field offices of federal law enforcement agencies, the relevant sector-specific agency, and several other authorities. Key resources and points of contact include the following:

- **Federal Bureau of Investigation (FBI)**
  Field Office Cyber Task Forces: www.fbi.gov/contact-us/field
  Internet Crime Complaint Center (IC3): www.ic3.gov
- **National Cyber Investigative Joint Task Force**
  NCIJTF CyWatch 24/7 Command Center: (855) 292-3937 or cywatch@ic.fbi.gov
- **United States Secret Service (USSS)**
  Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):
  www.secretservice.gov/contact/field-offices
- **U.S. Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)**
  HSI Tip Line: 866-347-2423 or www.ice.gov/webform/hsi-tip-form
  HSI Field Offices: www.ice.gov/contact/hsi
  HSI Cyber Crimes Center: www.ice.gov/cybercrimes
- **National Cybersecurity and Communications Integration Center (NCCIC)**
  NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov
  United States Computer Emergency Readiness Team: www.us-cert.gov

Public Relations and Other Communications

The WIRP may designate one or more individuals from the IR Team or another department to handle press releases and other public announcements, if needed. This individual should be responsible for determining whether any public communications are recommended, and if so, the timing and content of such communications. All public communications should be reviewed by the legal counsel and the IR Team. Consider whether this individual or another member of the IR Team should also handle internal communications to alert leadership and, if required, to explain the incident to employees.

Recovery and Follow-up

After resolution of the incident, conduct a review to assess the response and to discuss whether additional measures should be implemented to help prevent a similar incident from occurring. These additional measures may involve updates to your organization's security systems or updates to the WIRP and your other policies and procedures.

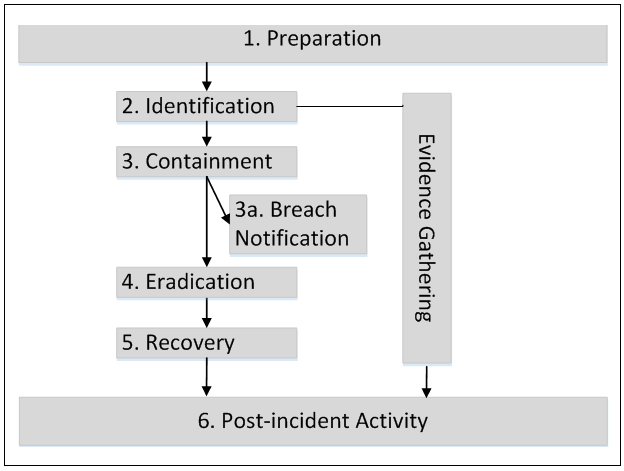
Sample Language

Within [one week] of the resolution of a data security incident, the IR Team will reconvene along with others who participated in the response, to conduct a post-incident review. The post-incident review will include evaluation of the effectiveness of detecting and responding to the data security incident, identifying any gaps or places for improvement. The review should also include recommended actions to minimize the risk of reoccurrence. All these findings should be documented in a report. The IR Team, or its designee, should monitor and coordinate the completion of the recommended action items identified during the post-incident review process.

Response Plan

Responding to a cybersecurity related issue progresses through the phases listed below. These phases are noted in the Incident Handler's Handbook provided by SANS Institute[3], and supported by the National Institute of Standards and Technology (NIST) Special Publication 800-61[4], and include breach notification requirements. Figure 1 summarizes the Response Phases

Figure 1 – Response Phases



Phase 1 – Preparation: During this phase, ensure essential items are in place. A successful incident response will require proper manpower, training, tools, equipment. Make sure standing orders are in place to implement established response plans.

[3] Available at: www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

[4] Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Phase 2 – Identification: During this phase, identify and attempt to get clarity on the cybersecurity related issue. If at any point, the organization is confident a malicious event has occurred or is on-going, leadership should immediately reach out to WBD and CyberESI for guidance through the next phases.

Phase 2a – Watch and Learn: In certain situations, the organization may not have enough data to gain clarity on the scope of the compromise. Attempts to move to the containment phase can alert the adversary. By observing the incident via log monitoring and packet analysis, organizations may be able to gain much needed insight regarding the event.

Phase 3 – Containment: During this phase, efforts revolve around short-term containment to minimize or limit the amount of damage to the organization. System and related data must be preserved for investigative purposes. Long-term efforts to address the specific conditions that led to compromise (e.g., system patching, restricting unauthorized or compromised accounts, antivirus cleanup) should be noted.

Phase 3a – Breach Notification: Once detailed information regarding the event have been identified, which may include confidential information, breach notification laws may apply.

Phase 4 – Eradication: In this phase, systems are cleaned and returned to operations, any disk images are updated to ensure the conditions that led to the event are eliminated. Forensic related actions may be performed to ensure all steps have been taken to remove the threat vector, malware, and unauthorized configuration modifications.

Phase 5 – Recovery: This phase targets the return to normal operations. Relevant systems have been cleaned and mitigation strategies have been deployed. Policies, processes and procedures are updated if required.
CYBER DISRUPTION – CONTINGENCY PLAN - 20

Phase 6 – Post-Disruption Activity: This phase focuses on litigation support, lessons-learned from the incident response and the actual incident. Organizations should identify areas for training/exercise and updating incident response plans.

Cybersecurity related events involve many issues that may not be present in other types of network incidents. These include:

- Cybersecurity-related events can be difficult to detect, and false positives are common. The Identification phase is intended to ensure that potential events are being interpreted correctly.

- The individual or group conducting the attack will attempt to maintain access to the systems and disrupt the response efforts. Removing the adversary's access to environment is critical and requires an experienced approach.

- Gathering evidence in a proper fashion shall be conducted in all phases in the event that legal action is required.

Attachment A

Assessment Management & Risk Assessment Table

Function	Category	Subcategory
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value

		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources
		ID.RA-3: Threats, both internal and external, are identified and documented
		ID.RA-4: Potential business impacts and likelihoods are identified
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		ID.RA-6: Risk responses are identified and prioritized

About Us

Womble Bond Dickinson

Successfully managing cybersecurity and data privacy risks are first-order challenges for most organizations. Our multi-disciplinary cyber and data privacy team comprises more than 20 lawyers in the U.S and 20 in the UK who practice data privacy law across a broad range of sectors including the financial, technology, manufacturing, professional service, health care, education, telecommunications, utility and governmental sectors. We have in-depth knowledge of the NIST cybersecurity framework, current cyber law and insurance requirements and appropriate response strategies. Our U.S. cybersecurity team includes communications lawyers working on the specific data privacy and security concerns of regulated telecommunications, broadband and wireless companies as well as data privacy attorneys focused on the technology sector. Additionally, we have the support of a cyber defense technology firm that strategically partners with us to improve IT practices to prevent cyberthreats and mitigate the damage when threats become reality.

This guide came into being as we saw many of our clients experience similar challenges in dealing with cybersecurity and data privacy. While the challenges of the past are becoming more manageable, the challenges of the future are getting more complex. We hope this guide and plan can help you.

The Team

Carri Bennet | Partner | Washington, DC
e: carri.bennet@wbd-us.com
t: 202.857.4519

Carri has more than 30 years of experience advising telecom clients on regulatory issues, with a particular focus on serving rural wireless and broadband companies. She represents her clients before the FCC, state regulatory agencies, the courts and Congress. Carri works on cybersecurity compliance, risk management and crisis management issues with her clients to reduce the fallout and damages associated with a cyber incident.

Ted Claypoole | Partner | Atlanta, GA
e: ted.claypoole@wbd-us.com
t: 404.879.2410

Ted leads Womble Bond Dickinson (US) LLP's privacy and cybersecurity team and FinTech team, and he chairs the Cyberspace Law Committee in the business law section of the American Bar Association. He has long concentrated on the business and legal implications of information security and computer crime, first as in-house corporate counsel for CompuServe Inc. and as assistant general counsel for Bank of America. He served on a U.S. Justice Department task force on computer crime, and he still works with the FBI and Secret Service on computer crime issues.

Tara Cho | Partner | Raleigh, NC
e: tara.cho@wbd-us.com
t: 919.755.8172

Tara chairs Womble Bond Dickinson (US) LLP's privacy and cybersecurity team. Her practice is dedicated to counseling clients on privacy and data security issues across industries such as technology, retail, e-commerce, healthcare / health tech and life sciences. Tara became certified as a legal specialist in privacy and information security law by the North Carolina State Bar Board of Legal Specialization in 2018 as part of the inaugural class of specialists in this field. She is also recognized by the IAPP as a certified information privacy professional for both the U.S. (CIPP/US) and Europe (CIPP/E).

Marjorie Spivak | Partner | Washington, DC
e: marjorie.spivak@wbd-us.com
t: 202.857.4538

Marjorie represents telecommunications providers across the United States advising them on all aspects of policy, transactional, and regulatory compliance. Marjorie works with clients on cybersecurity matters including helping them to develop a cybersecurity incident response plan to provide awareness, and to prepare them to react and effectively recover in the event of a cybersecurity incident.

Nadia Aram | Of Counsel | Raleigh, NC
e: nadia.aram@wbd-us.com
t: 919.755.2119

Nadia focuses her practice on licensing/commercial contracts, privacy and advertising. She takes pride in helping clients advance business interests practically and creatively. Clients look to her to help buy and sell a variety of services, goods and software and to monetize IP, technology and other assets through licensing, including franchising and other co-ventures.

The Firm

Womble Bond Dickinson is a transatlantic law firm with more than 1,000 lawyers based in 27 US and UK office locations. The firm provides core legal services, including commercial, corporate, employment, pensions, dispute resolution, litigation, finance, banking, restructuring, insolvency, IP, communications, technology and data, private wealth, projects, construction and infrastructure, real estate and regulatory law. Learn more about us on our website at **www.womblebonddickinson.com**.

Cyber ESI

Focusing on the midsize enterprise with expanding cybersecurity needs, CyberESI offers a full range of information security services including incident response and digital forensics. CyberESI provides remote 24×7 security monitoring and management of your mission-critical networks. Expert staff also offers a range of professional services to assess your risks, establish the right security policies and procedures, and improve your overall security posture.

Joseph Drissel | CEO
e: jd@CyberESI.com
t: 410.921.3864

Joseph is the Founder and CEO of Cyber Engineering Services, Incorporated (CyberESI) - an industry leading managed cybersecurity services company. In this role, Joseph is responsible for all corporate vision, culture, and oversight.

In 2010, Joseph founded CyberESI to help organizations detect and respond to cyber threats and attack. Today, his team provides managed detection and response, incident response, and cyber threat intelligence to government and commercial clients, including the communications sector.

Before founding CyberESI, Joseph was the Acting Section Chief of the Intrusions Section at the Defense Cyber Crime Center's (DC3) Defense Computer Forensics Laboratory (DCFL), the world's largest accredited computer crime laboratory.

Joseph is also the co-founder of US CyberDome (https://uscyberdome.com/), a non-partisan non-profit dedicated to improving cybersecurity within political campaigns, party committees, and the community that supports them.

Joseph also serves as an authority in the cybersecurity and investigatory communities by providing his perspectives on CNN, Krebs on Security, and other media outlets.

Matt Barrett | Chief Operating Officer
e: mbarrett@CyberESI.com
t: 410.921.3864

Matt is Chief Operating Officer of Cyber Engineering Services, Incorporated (CyberESI, www.cyberesi.com) - an industry leading managed cybersecurity services company. Mr. Barrett oversees all facets of operation, including service oversight, client communications, employee well-being, and corporate operations.

Mr. Barrett is also the co-founder of US CyberDome (https://uscyberdome.com/), a non-partisan non-profit dedicated to improving cybersecurity within political campaigns, party committees, and the community that supports them.

Mr. Barrett previously led the Framework for Improving Critical Infrastructure Cybersecurity (a.k.a., Cybersecurity Framework; https://www.nist.gov/cyberframework) program for the National Institute of Standards and Technology (NIST). Through his awareness campaign and efforts, Barrett propelled the Cybersecurity Framework to world-wide use, with over 30% use amongst U.S. organizations (https://www.gartner.com/doc/3188133/best-practices-implementing-nist-cybersecurity).

Telcom Insurance Group

Telcom Insurance Group understands it is not enough to have the most knowledgeable and technically sound employees. They must take pride in their work and work as a team to provide their customer with an experience that is superior to that offered by the competition. Telcom Insurance Group provides relevant, up to date training to our team allowing them to be knowledgeable and an integral part of our client's risk management program. Learn more at **www.telcominsgrp.com**

Peter J. Elliott | CEO and President
e: pje@telcominsgrp.com
t: 301.784.6424

Peter is the CEO and President of National Telcom Corporation (NTC), which is a captive insurance company owned by the National Telecommunications Cooperative Association and a select group of its members. He hold the same role with Rural Trust Insurance Company, which is a traditional insurance company owned the same type of owners. Mr. Elliott joined National Telcom Corporation in October of 2000 as a Director of Program Development. He is learned business from the ground up as he rose to the level of President and CEO.

Peter has thirty-four years of experience working in the insurance industry. He has first-hand knowledge of mutual, stock, and captive insurance company operations and has also work directly for a national insurance trade association where he gained insights into the agency sector of the industry.

He earned his Charter Property and Casualty Underwriter (CPCU) designation in 1992. Peter has presented on insurance topics for the insurance, as well as for telecommunication industry and to independent agencies throughout the United States.