Cybersecurity and Data Security Best Practices

Insurance is a valuable tool in crafting a risk management program for many emerging and complex risks. Insurance for the cyber peril is no different. First and foremost, "cyber liability insurance" is a useful targeted risk transfer mechanism. Additionally, a well-crafted application and underwriting process can motivate a business to focus on individual risk assessments, encourage a top-down corporate culture of cyber risk awareness and compel the prioritization and implementation of risk-based security measures. Importantly, carriers frequently make available pre- and post-incident services. The pre- and post-incident services that may be offered are risk engineering and loss control tools that can include resources such as: access to pre-breach planning (i.e., developing and testing an Incident Response Plan or Disaster Recovery Plan); employee training and testing; vulnerability assessments; detection capabilities; penetration testing; loss prevention consultations; access control and protection capability technologies; data restoration tools; and ransomware, forensic and legal expertise.

Ransomware attacks are increasing in both frequency and severity as bad actors continue to evolve and adapt.

Ransomware attacks are increasing in both frequency and severity as bad actors continue to evolve and adapt. Criminal business models have emerged that allow individual bad actors to lease malicious software variants to multiple bad actors increasing the severity of the attacks, the impact, and harm to victims, and the potential financial gain to the perpetrators. Also, bad actors no longer just hold a system or information hostage but will exfiltrate data and threaten to expose that data if a stated sum of money is not paid. Further, recent disruptive events, such as the attack on Colonial Pipeline, evidence the significant risk ransomware presents to our national and economic security.

One component of a robust cyber risk management program is a liability policy which includes coverage for a cyber extortion event. Indeed, cyber liability insurance frequently includes reimbursement for the payment of ransom, but that is only one aspect of the policy. The pre and post-incident services noted above will also be available. In particular, the cyber insurer may help companies access services of ransomware specialist vendors who can quickly evaluate the likelihood of receiving decryption keys, the type of ransomware strain, the payment recipient and whether there is a potential sanctions nexus.

[T]he insurance industry has prepared recommended data security hygiene steps businesses and individuals can take to improve their cyber defenses.

In furtherance of its desire to assist society with its security practices, the insurance industry has prepared recommended data security hygiene steps businesses and individuals can take to improve their cyber defenses. The American Property Casualty Insurance Association ("APCIA") provides links to potential authoritative resources such as the National Institute of Standards and Technology ("NIST"), the Cybersecurity Infrastructure Security Agency ("CISA"), and the Federal Bureau of Investigation ("FBI") to name a few. These resources offer detailed recommendations to businesses and individuals who wish to shore up their cyber protections utilizing the latest information available.

continued

American Property Casualty Insurance Association℠
INSURING AMERICA apci.org

Firms may also want to consider implementing ISO 27000 information security standards into their operations. The ISO 27000 series of standards have been specifically reserved by The International Organization for Standardization ("ISO") for information security matters. ISO has published the following information security standards for potential use:

- ISO27000 Information technology: Information security management systems, Overview and vocabulary
- ISO27007 Guidelines for Information Security Management Systems Auditing
- ISO27008 Guidelines for ISM auditing with respect to security controls (approved April 2008)
- ISO27011 Information technology: Information security management guidelines for telecommunications
- ISO27033 Network Security
- ISO27799 Health Informatics: Information security management in health using ISO/IEC 17799

A link explaining the ISO 27000 standards is found **here**.

CYBERSECURITY BEST PRACTICES	LINKS/RESOURCES
A business should implement a risk-based information security program.	**NIST Cybersecurity Framework** **NY Cyber Regulation** **NY DFS Guidance on MFA**
At a minimum the program should include the following high-level elements: Recover; Identify; Respond; Detect; Protect.	
The Information Security Program should be regularly reviewed and updated.	
Identify and regularly consult information sharing resources, such as CISA, that can help the company stay on-top of known vulnerability risks.	
Maintain an up-to-date inventory of all IT assets and regularly decommission systems that are no longer needed.	

MULTIFACTOR AUTHENTICATION (MFA) What does MFA mean; How do you determine when it is needed — what are the biggest risks and why won't compensating controls work as an alternative?	LINKS/RESOURCES
Businesses should apply multi-factor authentication (MFA) that requires at least two authentication events to protect against unauthorized access to non-public information or information systems.	**NIST 800-63** **NY Cyber Regulation** **CISA Ransomware Guide** **FBI Protected Voices: Passphrases and MFA** **FTC Basics: Cybersecurity for Small Businesses** **NSC Open Letter to Businesses** **CISA Bad Practices** **NY DFS Guidance on MFA** **CISA/FBI Holiday Guidance**
Authentication events fall into three categories: something you know (password or PIN); something you like (token or fob); something you are (fingerprint). Security questions are not an MFA authentication event.	
Single factor authentication is egregious for technologies accessible from the internet.	
Use MFA for cloud-based services, remote access, and administrative accounts.	

continued

BACK-UP MANAGEMENT	LINKS/RESOURCES
Businesses should maintain back-ups of all essential information that are kept isolated from the network and/or off-site (or on the cloud). An asset inventory can help identify what information is essential and where the information is stored.	**FTC Ransomware Guidance** **CISA Fact Sheet** **NSC Open Letter to Businesses** **SBA Top 10 Best Practices**
Back-up procedures should be identified and tested.	
Keep back-ups current – Back-up automatically if possible, or at least weekly.	
Air-gap (or other sufficient controls).	

PASSWORD PROTECTION	LINKS/RESOURCES
Maintain a policy that prohibits use of known/fixed/default passwords and credentials.	**CISA Bad Practices** **CISA/FBI Holiday Guidance** **NIST Password Guidance** (publication reference embedded in this article) **CISA Security Tip – Good Security Habits**
Mandate employees use strong passwords and prohibit reuse of a password across multiple accounts.	
Passwords should be long and complex (length is preferred).	
Require password resets only if the business suspects the password has been compromised.	
Set account lockout at 3-5 failed password attempts.	

PATCH MANAGEMENT	LINKS/RESOURCES
The business should have a patch management program in place. At a minimum it should include testing, validation processes, and deployment practices.	**FBI Ransomware Prevention and Response for CISOs** **NIST CSRC Guide to Enterprise Patch Management Technologies**
Deploy enterprise patch management tools in a phased approach.	
Keep patch management tools tightly secured and up-to-date; encrypt network communications, verify the integrity of patches before install and test before deployment.	

TESTING (pre-breach/incident response)
Utilize penetration testing and incident response testing.
Testing should be performed periodically and inform updates to the information security program and protocols as appropriate.

continued

TRAINING	LINKS/RESOURCES
Businesses should implement employee awareness training (including suspicious link training and regularly remind employees not to click on the suspicious links).	**FBI Ransomware Prevention and Response for CISOs** **NY DFS Guidance on MFA**
Train employees on the importance of MFA and urge timely implementation of company MFA requirements – track and enforce compliance.	

DETECTION TOOLS	LINKS/RESOURCES
Implementing integrity monitoring that will allow the business to detect changes and deletions.	**NCCOE security guidance tools**
Incorporate event logging that can generate alerts.	
Detection tools should be part of the before system attachment and should that fail after attachment downloads to a system.	
Deploy containment tools.	

NETWORK SEGMENTATION	LINKS/RESOURCES
Segment and segregate networks based on role and functionality using virtual segregation or physical segregation.	**CISA Security Tip – Securing Network Infrastructure Devices**
Limit unnecessary lateral communication between networks.	

3RD PARTY RISK MANAGEMENT	LINKS/RESOURCES
Develop due diligence practices and contractual provisions that the company can monitor the cybersecurity practices and overall hygiene of critical vendors.	**NY DFS SolarWinds Report** **NY DFS Guidance on MFA**
Require MFA or a reasonably equivalent or more secure access controls for all 3rd parties accessing info systems with nonpublic information.	

ENCRYPTION	LINKS/RESOURCES
Encrypt data in transit over external networks or use alternate compensating controls.	**NY DFS Cyber Regulation**
Encrypt data at rest if feasible or use alternate compensating controls.	

continued

DATA MAPPING

Collection and storage locations of data – conduct analyses of data collection, storage, transfer of data in motion and at rest. Understand the movement of data in order to ensure security of the data.

ENDPOINTS AND DEVICE MANAGEMENT

Policies and procedures for smart devices

Laptop/desktop management

Removeable media policy

NETWORK MANAGEMENT

Wired and Wireless access and controls

Remote access – VPN

Cloud storage

PHYSICAL PLANT

Headquarters and Branch security

Data centers

Outlets

APPLICATION SECURITY

Web apps

Mobile apps

LINKS/RESOURCES

NIST Small Business Information Security: The Fundamentals

Wi-Fi - WFA2 compliant and certified system in place