CYBER SECURITY FOR CONTRACTORS:

WHAT YOU NEED TO KNOW ABOUT CYBER THREATS & SOCIAL MEDIA ATTACKS

Stephen E. Yoch
Felhaber Larson
220 South Sixth Street, Suite 2200
Minneapolis, Minnesota  55402
(612) 373-8559
syoch@felhaber.com
# TABLE OF CONTENTS

I. What is Cyber Security? ........................................................................................................... 1  
   A. Definition ............................................................................................................................. 1  
   B. Three Key Elements in Cyber Security. ................................................................. 1  
   C. Understanding Information Security............................................................................ 1  

II. What is the Threat? ................................................................................................................. 2  
   A. Only BIG Retailers, Utilities, Banks, and Hospitals, Right?–“I’m a Little Fish” ............... 2  
   B. There are Big and Increasing Risks Out There for Everyone ....................................... 5  
   C. Reasons for Hope.............................................................................................................. 5  

III. Source and Type of Threats. .............................................................................................. 6  
    A. Who is Initiating the Attacks ......................................................................................... 6  
    B. Internal Threats .............................................................................................................. 6  
    C. Common System Vulnerabilities. ................................................................................... 7  
    D. Type of Attacks.............................................................................................................. 7  
    E. A Closer Look at Ransomware ...................................................................................... 9  
    F. What About the Cloud? ............................................................................................... 12  

IV. Legal Landscape ................................................................................................................ 13  
   A. Legal Standard for Cyber Protection ................................................................. 13  
   B. Board Exposure ............................................................................................................ 14  
   C. Duty to Disclose a Breach......................................................................................... 14  
   D. Regulatory Fines and Sanctions .............................................................................. 15  

V. Limiting the Risk ................................................................................................................ 15  
   A. Contracting to Limit the Threat. .............................................................................. 15  
   B. Capital and Administrative Investment. .................................................................... 19  
   C. Risk Assessment ...................................................................................................... 21
D. Incident Response Plan .............................................................................................................21

VI. Responding to a Breach ........................................................................................................23
   A. Technical/System Phases of an Incident Response .........................................................23
   B. Look to Your Incident Response Plan ...........................................................................24
   C. Act Immediately to Limit Damage and Mitigate Exposure and Expense ....................24
   D. Determine if Internal or External Attack .......................................................................24
   E. Preservation of Evidence .................................................................................................24
   F. Engage Outside Legal Counsel ......................................................................................25
   G. Retain an Expert to Provide an Objective and Outside View ........................................25
   H. Determine Whether Law Enforcement Needs to be Notified .......................................25
   I. Determine Whether a Public Announcement is Required ..............................................26
   J. Determine Whether Notification to an Insurer is Required .........................................26
   K. Examine Software and Hardware to Determine Whether the Network is “Clean.” ....26
   L. Engagement in a Forensic Examination of the Causes of What Occurred ....................26

VII. Responding to Social Media Attacks ..............................................................................27
    A. Proactive Measures .........................................................................................................27
    B. Combatting an Attack .....................................................................................................28
    C. Conclusion ......................................................................................................................32

VIII. 10+ Tips to Staying Safe ..................................................................................................32
I. WHAT IS CYBER SECURITY?1

A. Definition. Measures taken to protect computers or computer systems against unauthorized access or attack.2 This can involve attacks against both computers as well as critical technology infrastructure.3

B. Three Key Elements in Cyber Security.4

1. Prevention. The ultimate goal of cyber security is to prevent an incident or a breach from occurring. Preventing cyber security breaches begins with establishing a plan and budget. Following best practices requires stating goals to the entire organization and assessing current risks. Finally, applying lessons learned to secure systems, networks, and applications with a strategy to prevent every attempted security violation.

2. Detection. Incidents begin as events and activities that show up on system and network logs. The ability to detect, alert, and “see” malicious cyber activity is often referred to, in the cyber security context, as “visibility.” An organization should actively look to improve visibility and adapt its detection environment to meet the constantly evolving threat vectors. Enhanced cloud-service provider visibility has contributed to a modest reduction in the American median dwell time, falling from 75.5 days in 2017 to 71 days in 2018.5

3. Response. Traditional security practices call this Incident Response. This effort now requires some level of forensics capability that includes methods beyond a technical approach by meeting legal standards and compliance, so this can also be called a Forensics Response. The inclusion of a forensic approach to handling incidents will ensure that the impacted company has documented a defensible process to demonstrate the company met its legal obligations as well as keeping the business operating securely. Companies must strategize to respond to every event with regular scheduled organizational meetings to make informed decisions.

C. Understanding Information Security.

---

1 Sections of this Article were drafted as part of a joint presentation conducted by Stephen Yoch with Calvin Weeks of Eide Bailly, entitled: The Eye of the Storm: Preparing for the Next Cyber Security Incident (June 6, 2017).
3 Department of Homeland Security Website.
5 FireEye Mandiant Services, M-Trends; Special Report, p. 7 (2019).
1. **Definition.** Information security is defined as the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, against denial of service to authorized users.

2. **“C.I.A. Triangle.”** Information security turns on the “C.I.A. Triangle” – Confidentiality, Integrity, and Availability.\(^6\)

   **Confidentiality:** The principle that objects are not disclosed to unauthorized subjects.

   **Integrity:** The principle that objects retain their veracity and are intentionally modified by authorized subjects only.

   **Availability:** The principle that authorized subjects are granted timely access to objects with sufficient bandwidth to perform the desired interaction.

Inherent in this business process is a balance between access and security, and for users, the balance between convenience and productivity. It is a constant struggle to protect data, but when the right balance is reached it can work very well for everyone. The “C.I.A. Triangle” discussed above can be analogized to a “real world” example outside the IT environment. For example, emergency first responders must have resources available that in many cases are confidential and only available to authorized emergency professionals such as police, fire, and paramedics (this is akin to the “CONFIDENTIALITY” part of the C.I.A. Triangle); the resources for first responders must be accurate and up-to-date (“INTEGRITY”); and the resources must be both available 24 hours a day 365 days per year, and quickly available to emergency professionals serving the people of their community (“AVAILABILITY”). If any one of the C.I.A. Triangle principles fails or gets out of balance, then the results could literally mean life or death for real people. Likewise, failure to maintain an appropriate balance of confidentiality, integrity, and availability can result in either important information not being immediately available and accessible to the business, or a security breach for lack of adequate diligence.

II. **WHAT IS THE THREAT?**

   A. **Only BIG Retailers, Utilities,\(^7\) Banks,\(^8\) and Hospitals, Right?—“I’m a Little Fish”**.

\(^6\) CIA Triangle is an essential security principle for ISC2.org common body of knowledge for CCSP and CISSP certifications.
1. **The Construction Industry.**

   a. There have been major construction industry security breaches. Use of Building Information Modeling and Virtual Project Management software have made construction projects increasingly vulnerable to cyber security attacks. Central Concrete Supply Company in California, and Century Fence in Wisconsin, were both recent victims of phishing attacks. A management company in Vallejo, California suffered a ransomware attack in March, and most notably, Turner Construction Company, a large national construction company, suffered a breach in April, releasing personal information on its 5,600 employees.

   b. One recent study noted that the highest percentage of phishing attacks, including spam, went to construction-related industries.

   c. Many people believe that the construction industry is less vulnerable because it deals more with “tangible items” rather than digital information which is typically the subject of a cyber security attack. However, construction companies have increasingly created virtual construction tools for design, project management, and customer tracking. In an increasingly automated environment, payment information, designs, and customer information are ripe for cyber attack and, in particular, ransomware breaches.

   d. 30% of real estate executives with one or more properties have experienced a cyber security event in the last two years, and 50% of the real estate industry says their organization is not adequately prepared to mitigate a cyber security attack. Yet, only 5% of respondents noted cyber security threats as a serious risk to their business.

   e. 77% of executives in the construction, engineering, and infrastructure industry said they have experienced a cyber security incident in the last 12 months.

   f. Ex-employees were responsible for a third of all cases of fraud. The most common targets for cyber security attacks against construction companies were customer records, employee records, and physical assets/money.

2. **Small Businesses are Vulnerable.**

---

7 Utilities, for example, are a major target for cyber intrusion. A recent study sponsored by the U.S. Government focused on this very issue, Mission Support Center Idaho National Laboratory, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector (August 2016).

8 FireEye Mandiant Services, M-Trends; Special Report, p.9 (2019) (23% of the firm’s investigations involved the financial industry).
a. There is a significant gap between large and small businesses and their approaches to cyber security incidents. 62% of larger companies say that practicing their crisis communications in response to cyber security incidents is a high priority, while only 47% of small companies say the same thing. Significantly, the cost per incident is approximately the same for small and large companies on a per employee basis. The result is small firms’ complacency could mean their demise.

b. Small businesses are severely impacted by cybercrime each year; with one survey reporting that 43% of data breach victims in 2018 were small businesses.

c. “One mistake often made by these small businesses is to assume that they cannot be targeted, thereby making them easy targets. Hackers are aware that these small enterprises lack the resources, experience or policies to fight them.”

d. Small businesses hold consumer and employee information, making them prime targets. Information that hackers target ranges from on-line banking credentials to social security numbers.

e. There are two primary reasons hackers are increasingly going after small businesses: (1) Small businesses are plenty in number and present a huge market for exploitation; and (2) Larger enterprises have enhanced their security systems and have pushed hackers to look for easier targets.

f. The lower costs of computing power allow bad actors to develop malware that permits more sophisticated attacks with greater frequency, a trend which is fueled by an illegal market for malware development kits.

g. Small businesses are moving to the cloud. The overall cloud market for small and medium sized businesses continues to grow, with significant associated risks.

h. Companies with fewer than 250 employees have the highest malicious email rate.

i. 53% of mid-market businesses (250-499 employees) say they have experienced a cyberbreach, and 20% of these businesses have reported that these breaches cost them between $1 million to $2.5 million.

---

B. There are Big and Increasing Risks Out There for Everyone.

1. According to Risk Based Security’s Data Breach QuickView Report, there were 4,149 data breaches compromising over 4.2 billion data records in 2016. This represented an all-time high and included the Yahoo data breach, which, at over 1 billion records, was the single largest breach ever disclosed.

2. 91% of organizations experienced at least one cyber security incident in the past year.\textsuperscript{14}

3. 44% of organizations experienced more than 25 cyber security incidents in the past year.\textsuperscript{15}

4. Over a quarter of organizations that have suffered from a security breach and lost business. Four in ten said those losses were substantial.\textsuperscript{16}

5. A Ponemon study estimates the probability of a data breach in the next two years at 27.9% (an increase from 2017).\textsuperscript{17}

6. Six of the 2016 breaches rank among the ten largest of all time.\textsuperscript{18}

7. Cost of data breach:
   a. Average cost of a data breach was $3.86 million;\textsuperscript{19}
   b. $148 per record exposed. Id.
   c. Data breach is detected and contained in an average of 69 days.\textsuperscript{20}

C. Reasons for Hope. A 2019 SANS Institute survey showed that 81% of its respondents that were utilizing cyber threat intelligence (CTI) as a means for prevention, detection, and response to cyber attacks believed their organizations had an increased ability to prevent and detect cyber security intrusions. Unfortunately, 17% of that same group did not know the extent that their prevention or detection capabilities had actually improved. The primary improvement identified was better visibility to threats and

\textsuperscript{13} Sean Teehan, Tech Gains, Cyber Pains, Minneapolis/St. Paul Business Journal, p. 12 (July 5, 2019).
\textsuperscript{14} Matt Bromiley, SANS Institute, It’s Awfully Noisy Out There; The 2018 SANS Incident Response Survey p. 3 (October 2018).
\textsuperscript{15} Matt Bromiley, SANS Institute, It’s Awfully Noisy Out There; The 2018 SANS Incident Response Survey p. 3 (October 2018).
\textsuperscript{17} Ponemon Institute, 2018 Cost of Data Breach Study: Global Overview, p. 3 (July 2018).
\textsuperscript{19} Ponemon Institute, 2018 Cost of Data Breach Study: Global Overview, p. 3 (July 2018).
\textsuperscript{20} Ponemon Institute, 2018 Cost of Data Breach Study: Global Overview, p. 4 (July 2018).
understanding of attack methodologies. Lack of trained staff continues to be the biggest inhibitor to cyber security.\textsuperscript{21}

III. SOURCE AND TYPE OF THREATS.

A. Who is Initiating the Attacks? As never before there are “state actors” engaging in aggressive cybercrimes. The Chinese, Russian, Iranian, and North Korean governments are all major actors.\textsuperscript{22} Professional syndicates are located in haven countries like Russia, Ukraine, and the Philippines. Indeed, the sophistication of criminal syndicates has reached such a level that the line between state actors and cyber criminals has largely blurred.\textsuperscript{23} There is often a tacit agreement between the host country and the cyber criminals that cybercrime will not be committed within the host country’s national borders.

B. Internal Threats.\textsuperscript{24} Negligent insiders caused 27\% of data breaches, while malicious insiders and criminal hackers caused 48\% of all data breaches.\textsuperscript{25} “Malicious insiders” are the largest source of cyber security threats, and this threat has been increasing year after year. The activities of malicious insiders have the third highest annualized cost to companies behind malware and web-based attacks, respectively.\textsuperscript{26} Internal threats stem from the following problems:

1. Lack of diligence in hiring. This is much more than a thorough background check and has less to do with technology.\textsuperscript{27}

2. Lack of training. Awareness training is the minimum that should be provided to all staff. Training should include reporting of security and policy violations.

3. Lack of employee monitoring. Organizational wide monitoring of all employees for their own protection will help businesses identify anomalies in normal activity patterns, first as a group and then individually.

4. Lack of guarding from former employees. Even after all access has been removed and accounts have been disabled, does the company have a way to monitor attempts to access? How about monitoring public internet and social

\begin{thebibliography}{26}
\bibitem{25} Ponemon Institute, \textit{2018 Cost of Data Breach Study: Global Overview}, p. 9 (July 2018).
\bibitem{26} Accenture and Ponemon Institute, \textit{The Cost of Cyber Crime: Ninth Annual Cost of Cybercrime Study}, p. 20 (March 2019).
\bibitem{27} Due Diligence Checklist from Employment Screening Resources, www.esrcheck.com (July 2010).
\end{thebibliography}
media for public comments and activities that could be negative or leak confidential information?

C. Common System Vulnerabilities.

1. Unsecured communications. Systems have been designed to maximize efficient communications within a network. However, this creates vulnerabilities that allow eavesdropping on unencrypted communications across wireless and wired networks permitting attackers to masquerade as trusted users to hijack all or a portion of a system.

2. Mismanaged user access credentials. Hackers often are able to obtain access through use of “guessing” or otherwise using brute force attacks to obtain logins and passwords. Individuals are often tricked into providing their credentials through phishing attacks. Eavesdropping on unsecured communications can also result in passwords being detected. Also, passwords of terminated employees are often left active and open resulting in vulnerability either inadvertently or deliberately by disgruntled employees. Even factory defaults can be used as a “back door” into computer systems.

3. Unsecured configurations. Software and hardware can be installed in a way to permit access to IT systems, but these factory default settings can also leave vulnerabilities to the system. Strong authentication firewalls need to be installed around hardware and software at the time of installation.

4. Unpatched vulnerability. The cyber security environment is constantly changing and IT professionals need to invest in updating patches, hardware, and software to minimize vulnerabilities. This is an ongoing process. Failure to patch vulnerabilities can result in infiltration of systems.

D. Type of Attacks. Virtually all attacks involve some amount of “malware” being inserted into the target computer system. The total amount of malware on the web continues to rise steadily, with mobile-related malware rising at an even greater rate. This attacking software (a/k/a malware) includes trojan horses, viruses, rootkit, 


31 McAfee, McAfee Labs Threats Report, p. 70-71 (June 2017).

32 Trojan horses often appear to perform desirable functions, but actually contain undisclosed malicious software. This is code that masquerades as a benign application. Once the program is inside the system, the malware is unleashed in the system. This is distinct from a virus, as a trojan horse does not replicate itself.
spyware, botnet, and worms and is usually introduced into systems through e-mail attachments or downloads. Malware often involves code masquerading as “good” software or code that attaches itself to “good” software. The ultimate goal of the attacker is to gain enough access to the systems and networks to setup an account that would hide itself and create other authorized accounts for use. That way when the malware is discovered, but is only cleaned from a system, the hacker still has access through accounts that are setup on the system that look and function the same as any other user. This is why systems and networks should always be rebuilt and not just cleaned after a compromise.

1. **Point of sale intrusions.** Some malware is inserted into a retailer’s credit card processing system to collect credit card data and forward that account information to the attacker.

2. **Phishing attacks (a/k/a “Spear Phishing”).** E-mail which pretends to be from a trusted party or otherwise induces or tricks an e-mail user to click on a link or an attachment. Malware is then deployed.

3. **Password attacks.** Trying to gain passwords through cracking of codes or other unsavory means. Rainbow tables nearly ensure that passwords alone can never be trusted to protect from attack or compromise.

4. **Man in the middle.** Someone impersonates another in an information chain. This often involves sending requests for information or monetary wire payment. Usually access is made through non-encrypted wireless access points and networks.

5. **Drive-by download.** Malware exists on a legitimate site. Just by visiting the site a code is downloaded into the user’s site which then reaches out to another computer to get the rest of the download.

---

33 A computer virus is a virus that typically is capable of copying itself and is designed to spread within the host computer, system, or network environment. The virus may corrupt or delete data on a computer system, or use e-mail programs to cause the virus to spread to other computer systems.

34 A rootkit is a type of software designed to hide in an operating system. It is often used to permit unauthorized parties access to a computer system without detection. This is often known as a “hide in plain sight” software program.

35 Spyware is software that gathers information without the user’s knowledge and routes it back through the internet to the attacker.

36 A botnet is a collection of off-sam computers that have been taken over by malware. Each compromised computer is called a “bot.” The command of these compromised systems is used to control the “botnet” under the direction of a “botmaster.”

37 A computer worm is a standalone form of malware that uses a computer network to spread. Like a virus, it replicates itself. However, unlike a virus, a worm does not need to be attached to an additional program. The distinction between a virus or Trojan horse and a worm is that a worm can spread without human interaction.
6. **Malvertising.** Cyber attackers upload infected ad displays on different sites. The ads look legitimate but in fact constitute a form of malware to attack the user.

7. **Rogue security software.** Designers make pop-up windows look like alerts concerning possible security threats. Users then inadvertently provide information which worsens the security vulnerability of their systems or tricks the user into providing sensitive information.

8. **Theft of laptops or mobile devices.** Unencrypted or inadequately encrypted mobile devices are a significant source of both data loss and create potential vulnerabilities to associated networks.

9. **Ransomware.** Malware is introduced into the system where the system can be shut down, disabled, or held hostage.\[38\] This is sometimes called “ransomware.” The wrongdoer demands “ransom” be paid before a restriction on the computer system is removed. The encryption used on ransomware is incredibly powerful. “Typical ransomwares software uses RSA 2048 encryption to encrypt files. Just to give you an idea of how strong this is, an average desktop computer is estimated to take around 6.4 quadrillion years to crack an RSA 2048 key.”\[39\]

E. **A Closer Look at Ransomware.** Businesses are increasingly targeted by ransomware. While 2018 saw an overall decrease in ransomware infections, enterprise ransomware attacks increased by 12 percent, resulting in an 81 percent share of all ransomware attacks.\[40\] One report noted that business ransomware detections in Q1 2019 increased by 195% when compared to the previous quarter.\[41\] This shift towards targeting business illustrates a heightened area of focus for cybercriminals, and accordingly consumer attacks have fallen by 10 percent over the same period.\[42\] The number of enterprises experiencing ransomware attacks has more than tripled over the last two years.\[43\]

\[38\] In one recent survey, denial of service type attacks represent 55% of all cyber security incidents. SANS Institute, *The Show Must Go On! The 2017 SANS Incident Response Survey*, p. 8 (June 2017); Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview*, p. 3 (June 2017) (The average number of days to identify data breach is 191 days).


1. **Costs.** The costs associated with a ransomware infection are high. Although it is not recommended, victims who decide to pay the ransom to decrypt data spent an average of $6,733 per attack during the fourth quarter of 2018.\(^{44}\) Enterprises incur great expenses when recovering from the consequences of a ransomware attack. The average annual cost of a ransomware attack in 2018 was $645,920.00, rising 21% from the previous year.\(^{45}\)

2. **No expertise needed.** Ransomware attacks will remain prevalent with the proliferation of Ransomware-as-a-Service (RaaS) offerings, where an individual with the intent to launch an attack can purchase ransomware code written by another cybercriminal, typically for less than $500.\(^{46}\) Further contributing to the spread in ransomware attacks are ransomware construction kits, which allow novice hackers and low-skilled cybercriminals to build ransomware variants.\(^{47}\)

3. **SamSam Ransomware.** While most ransomware utilize spam campaigns that indiscriminately target businesses and consumers, SamSam ransomware is used against specific organizations, including hospitals and schools, that are most likely to pay to decrypt their data.\(^{48}\) Nearly a quarter of the organizations hit by SamSam in 2018 were health care organizations.\(^{49}\) There has been evidence of at least 67 SamSam attacks in 2018, mostly against organizations in the U.S.\(^{50}\)

   a. Cybercriminals behind SamSam access the victim’s network by using brute-force tactics against weak passwords on machines accessible online using Remote Desktop Protocol [RDP].\(^{51}\) The group that operates SamSam has developed it privately and updates it frequently in order to avoid detection.\(^{52}\) The attacker deploys Mimikatz, a credential harvesting tool, as a mechanism to gain domain admin access.\(^{53}\)

---


\(^{48}\) Dorka Palotay and Peter Mackenzie, SophosLabs, *SamSam Ransomware Chooses its Targets Carefully*, p. 2 (April 2018).


\(^{52}\) Sophos, *SamSam Explained: Everything You Need to Know About This Opportunistic Group of Threat Actors* (April 18, 2018).

b. SamSam is distinct from other well-known ransomware (e.g. WannaCry) in that it does not have worm or virus capabilities. The attacker manually deploys SamSam using stolen credentials and Windows network administration tools as if it were a legitimate application. From this position inside of the server, the attacker manually selects targets to encrypt. Once the attack has been launched, a ransom note is displayed that typically states the victim has seven days to make a payment to the attacker’s dark web payment site in order to receive a decryption key.

c. SamSam ransomware attacked the City of Atlanta’s computer network in March 2018, with the attackers demanding around $51,000 worth of bitcoin. The City did not pay the ransom, and mitigation efforts as a result of the breach ultimately cost the city $17 million.

4. Ransomware Targets Backups. Ransomware attackers know that compromising a backup system is integral to influencing an enterprise’s decision to pay. The latest iterations of ransomware do not detonate right away. After spreading to as many systems as possible, the infection may be dormant for weeks or months. Backup systems see the malware as another file to be protected, so it is replicated in the backups. Once it is detonated and a ransom is solicited, the backups are used to recover the encrypted data. The ransomware is once again deployed, forcing the network administrator to go to an older backup, repeat the data recovery, and deal with the ransomware again, creating a “ransomware attack loop.” Because it is difficult to determine when the ransomware was backed up, the organization must balance the amount of data it is willing to lose with the costs of paying the ransom.

a. In Q4 of 2018, 75% of ransomware cases in one survey involved the wiping or encryption of primary and secondary backups.

b. To minimize the risk of ransomware compromising backups, the backups should not be visible to the computer, either as a drive letter or a network share. Industry best practices include archiving backups to

---

54 Id.
55 Id.
57 Kate Fazzini, CNBC, The Landmark Ransomware Campaign That Crippled Atlanta Last March Was Created by Two Iranians, Says DOJ (November 28, 2018).
59 Eran Farajun, Asigra, Why 3-2-1 Backup has Become an Ineffective Ransomware Defense (September 26, 2018).
61 Alastair Cooke, TechTarget, Cloud Backup Systems Are a Good Bet in Ransomware Fight (September 2017).
removable media such as tapes, optical disks, or removable hard
disks.  

F. What About the Cloud? 70% of midmarket companies hosted at least one network in the cloud. The use of the cloud for IT infrastructure is a source of grave concern for cyber security professionals. 54% of IT professionals surveyed indicated that their organizations do not have a policy that requires security safeguards (i.e. encryption) as a condition for utilizing cloud computing applications. The primary considerations for selecting a particular cloud provider are efficiency (42 percent of respondents) and cost (39 percent of respondents), while security concerns were a factor considered by only 23 percent of respondent’s organizations.

In its basic concept, the cloud provides Availability of the C.I.A. Triangle as its greatest potential, if nothing else is considered for cyber security. The misperception that “the cloud is more secure” is just a myth. Simply, “You can outsource the work, but you cannot outsource the risk.” Security principles of the C.I.A. Triangle must be applied to cloud operations the same as traditional infrastructures, but the technology and how it is applied is completely different and takes additional skill sets to secure.

1. Internal. An “internal” or “private” cloud involves an offsite location for servers. This is a location that serves only one user. These are usually available for large companies and provide secure service as long as the user has in place all of the other normal precautions and investment in security infrastructure.

2. External. “External” or “public” clouds are the “brave new world” of virtual computing. A public/external cloud involves using the infrastructure of third party servers to hold the user’s data. The key issue is the data is outside the user’s direct control.

The absolute key issue in a “public” cloud-based system is due diligence by the user. This analysis should include: (a) understanding the public server’s disaster and recovery systems; (b) employee security policies; (c) protection of data; and (d) (crucially) whether the cloud provider has certifications by recognized standards like National Institute of Standards and Technology (NIST), Statement on Standards for Attestation Engagements No. 16 (SSAE16), Service Organization Controls (SOC) 2 Type II, and International Organization for Standardization (ISO) 27001. Depending on the nature of

63 Christine Kent and Jane Irene Kelly, Cisco, SMB Cybersecurity Trends (March 4, 2019).
65 Id. at 14.
66 McAfee, McAfee Labs, 2017 Threats, Predictions, p. 12 (November 2016).
67 Cybercriminals are following the data and are levying more attacks against the cloud. See FireEye Mandiant Services, M-Trends: Special Report, p. 3 (2019).
customer data being kept on the cloud, some additional precautions may be necessary to avoid violation of state and/or federal law, including those required under Gramm Leach Billey Act (GLBA) and/or Health Insurance Portability and Accountability Act (HIPAA). Put another way, many people view using a cloud-based system as “simplifying” operations. Nothing can be further from the truth. A company must be more diligent in ensuring that its cloud-based vendor is engaged in adequate cyber security measures to protect company data.

3. **Hybrid.** A hybrid cloud involves using a mix of on-premises, private cloud, and/or third-party public cloud services in orchestration between the various platforms. Hybrid clouds are designed for use by one organization. The public and private sections must operate independently and communicate over an encrypted connection. What is key is that public and private clouds in a hybrid cloud are distinct and independent. This allows more sensitive and protected information to be stored on the private cloud.

**IV. LEGAL LANDSCAPE.**

A. **Legal Standard for Cyber Protection.** Companies must implement “appropriate” measures to protect data under federal law (e.g., GLBA and HIPAA). There are also significant industry-wide organizations and standards which impose legal obligations on companies handling credit cards, specifically the Payment Card Industry Data Security Standard (PCI DSS). Other relevant statutes include the Fair Credit Reporting Act (FRCA), the Children’s Online Privacy and Protection Act (COPPA), the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), the Telephone Consumer Protection Act (TCPA), the Telemarketing Consumer Fraud and Abuse Prevention Act, the Deceptive Mail Prevention and Enforcement Act, and the Computer Fraud and Abuse Act (CFAA). The Federal Trade Commission (FTC) retains substantial authority and has prosecuted disclosures of Personally Identifiable Information (PII). Many states also impose a requirement of “reasonable measures” to protect data. Most involve implementation of some Written Information Security Program (WISP) or following the requirements of NIST cyber security framework. Both involve a process by which a risk assessment is made, security standards and controls are developed, and physical, technical, and administrative controls are put in place. All standards involve five basic functional categories:

- Identifying the problem;
- Protecting data;
- Detecting intrusion;
- Responding to an incident; and
- Recovering from the incident.
B. **Board Exposure.** Cyber security is now a crucial issue in all corporate environments. As such, under the Business Judgment Rule, boards of directors have an enterprise-wide duty to assess and limit risk using best practices. Quite simply, this is no longer an “IT” issue. At a minimum, boards of directors need to:

- Understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue;
- Understand the legal implications of cyber risks as they relate to their company’s specific circumstances;
- Have adequate access to cybersecurity expertise;
- Have regular discussions about cyber-risk management that are given regular and adequate time on board meeting agendas;
- Set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget. In 2017, the majority of cyber security budgets increased (59%) over the preceding 12 months by at least 5% or more; and
- Have board management discussions about cyber risk that include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach. Failure of boards to act with the required duty of good faith care and loyalty could and likely may result in personal liability resulting from both regulatory action as well as shareholder lawsuits.

C. **Duty to Disclose a Breach.** Increasingly, state and federal authorities are requiring disclosure by companies in the event of a breach of the public’s sensitive personal information. This especially involves sensitive financial information (under the GLBA) or health and medical information (under HIPAA). Other privacy statutes

---


71 Heather King and Megan Stifel, “To Get Ahead of Cybersecurity Threats, Focus on Preparedness and Sustainability,” Navigating the Digital Age: The Definitive Cyber Security Guide for Directors and Officers, p. 201 (2d ed. 2018) (“Putting security first in all business operations enhances confidence in the processes that develop products and services, which results in better products and services that support the brand and ultimately leads to increased profits.”)

include the Fair Credit Reporting Act and Children Online Privacy Protection Act. The Securities and Exchange Commission (SEC) also requires disclosure of material events which “a reasonable investor would consider important to an investment decision.”\(^{73}\) PCI DSS similarly requires disclosure if there has been a breach of credit card information. Consultation with counsel is crucial in determining whether disclosure is necessary, and if so, the extent and timing of such disclosures (discussed below).

D. Regulatory Fines and Sanctions. Companies often suffer a “double whammy” as a result of a cyber security breach. Not only is there the cost of the breach itself (discussed below), adverse publicity, potential liability to customers, and remediation costs, but increasingly regulatory authorities are fining and penalizing companies for release of confidential or proprietary information. Such regulatory bodies include the FTC, SEC (Office of Compliance, Inspections & Examination), Financial Industry Regulatory Authority (FINRA), the Justice Department (enforcing claims under GLBA), the PCI DSS, and most severely sanctions by the Health and Human Services Department’s Office for Civil Rights (which handles HIPAA enforcement).

V. LIMITING THE RISK.

A. Contracting to Limit the Threat.

1. Third parties - Vendors. Third party involvement in a breach increases the cost. When a third party causes a data breach, the cost increases by $13 per compromised record.\(^{74}\) Thus, it is crucial that companies look not only to their own vulnerabilities, but also attempt to minimize risk caused by third-party providers and vendors.

   a. System and plan requirements. Simply imposing contractual obligations for indemnity (see below paragraph (b)) may be insufficient as the vendor may not have sufficient wherewithal to actually protect the indemnified party from risk. Thus, it is crucial that companies seek detailed information about the vendor’s security processes, firewalls, and encryption. This ideally should include the vendor’s own internal risk assessments, and whether or not the vendor has met the standards set by NIST, SSAE 16, or the ISO.

   For example, the following language is used by one Minnesota company requiring NIST compliance for its vendors:

   “NIST Compliance

   (1) Security of Confidential Information.
   Contractor, Contractor personnel, and third-party contractors

\(^{74}\) Ponemon Institute, 2018 Cost of Data Breach Study: Global Overview, p. 3 (July 2018).
shall safeguard and prevent the unauthorized disclosure of Company’s Confidential Information as defined in and in accordance with this Agreement. In addition to Section ___ of this Agreement, as it relates to Company’s Confidential Information shall take precedence over any conflicting provision in this Agreement.

(2) **Regulatory Compliance.** Contractor, Contractor personnel, and third-party contractors shall comply with applicable federal, state and local laws relating to the privacy, confidentiality or security of Company’s Confidential Information. Contractor, Contractor personnel, and third-party contractors shall only access and use Company’s Confidential Information as necessary to provide the Services.

(3) **NIST Compliance.** Contractor agrees that all systems and technologies of Contractor, Contractor personnel, and third-party contractors which store, transmit, create, or maintain Company’s Confidential Information conforms to the most recent NIST Cyber-Security Framework’s standards and controls (http://www.nist.gov/cyberframework).

(4) **Incident Notification.** Contractor shall promptly notify Company (but in no event more than forty-eight (48) hours after the occurrence) of any unauthorized access to systems of Contractor, Contractor personnel, or third-party contractors. Notification shall be communicated to the designated Company contact by telephone and subsequently via written letter and email of any successful security attacks or incidents to the extent Company Confidential Information is involved. The notice shall include the approximate date and time of the occurrence and a summary of relevant facts, including a description of the measures being taken to address the occurrence.

(5) **Verification of Breach Resolution.** Contractor shall provide contemporaneous updates relating to the corrective actions being taken to resolve any such data breach, in addition to mitigating action to prevent future similar data breaches from occurring. Company may request, and Contractor shall provide at no additional cost to Company, a third-party verification of such breach resolution before resuming or conducting future business with Contractor.

(6) **Security Accreditation.** Upon request by Company, no more than once per year, Contractor shall provide Company with a copy of its current certified SOC 2 type 2
Audit Report for systems of Contractor and Contractor personnel (or comparable industry-standard successor report prepared by independent third-party auditor).

(7) **Right to Audit.** Contractor agrees to cooperate with Company’s reasonable requests to perform a security audit, including, but not limited to, responding in good faith to reasonable requests to change or modify this Agreement as it relates to Company’s regulatory compliance; and providing documentation, including system audit information and incident response reports, to validate ongoing compliance by Contractor, Contractor personnel, and third-party contractors, with the security and confidentiality obligations hereunder.”

b. **Indemnity provisions.** Companies often demand indemnity from vendors which provide that the vendor shall “indemnify and defend” the company from any and all losses, damages, or risks as a result of a cyber security breach. Unfortunately, such broad indemnity obligations, while legally enforceable, do not protect the indemnified company from the harm to its business and reputation, and, in many cases, the vendor may simply be unable to meet the financial obligations and liability stemming from the promise contained in the indemnity.

c. **Privacy.** Some laws actually require clear agreements by and between parties to protect personal private information and vendors. For example, HIPAA requires that covered entities ensure HIPAA compliance in a Business Associate Agreement, and parties otherwise in possession of PII can also be subject to required contracts. Regardless, the sharing of “private” information places an enhanced duty to make sure information is protected when provided to vendors or third parties. In the event of any “breach” of private information, it is crucial that the vendor or third party be contractually obligated to immediately notify the impacted party.

d. **Right to audit.** All third party/vendors should be subject to a “right to audit” provision, which subjects any of their records, data or other information which may be impacted by the sharing of private, confidential, or sensitive system information to review.

e. **Testing and security review.** Vendors and third parties should be subject to penetration testing and security information reviews to insure system and data integrity.
2. **Insurance limitations.**

There is no “industry standard” cyber insurance policy. Companies that have insurance protection save on average $4.8 per record breached. As the nature of the cyber security threat evolves on almost a daily basis, insurance companies and their products are attempting to assess the risk and create appropriate coverages. Potential risks to be covered by cyber insurance include:

- Theft of money from accounts – direct money transferred;
- Ransom/extortion;
- Business interruption;
- Damage to software and hardware; and
- Public relations expense.

Cyber insurance is not comprehensive and usually contains significant limitations and deductibles. In any event, cyber insurance cannot be viewed as a substitution for implementing robust efforts to limit risk.

3. **Types of insurance coverages.**

a. **First party coverages:**

1) Crisis management. Generally covers “crisis management” expenses that typically follow in the wake of a breach incident, e.g., breach notification costs, creditor monitoring, call center services, forensic investigations, and public relations efforts.

2) Network interruption. Generally covers the organization’s income loss associated with the interruption of its business caused by the failure of computer systems/networks.

3) Contingent network interruption. Generally covers the organization’s income loss associated with the interruption of its business caused by the failure of a third party’s computer systems/networks.

---


76 Ponemon Institute, 2018 Cost of Data Breach Study: Global Overview, p. 22 (July 2018). Given that the cost per breached record is $148.00 (See Id. at 3), insurance related savings on average are not material and insurance cannot yet be viewed as providing meaningful protection for cyber attack losses.

4) Digital assets. Generally covers the organization’s costs associated with replacing, recreating, restoring, and repairing damaged or destroyed computer programs, software, and electronic data.

5) Extortion. Generally covers losses associated with cyber extortion, e.g., payment of an extortionist’s demand to prevent a cyber security or data privacy-related incident.

b. Third party coverages:

1) Privacy liability. Generally covers third-party liability, including defense and judgments or settlements, arising from data breaches, (e.g. the Target breach) and other failures to protect confidential and protected information.

2) Network security liability. Generally covers third-party liability, including defense and judgments or settlements, arising from security threats to networks. (e.g., inability to access the insured’s network because of a DDoS attack or transmission of malicious code to a third-party network).

3) Regulatory liability. Generally covers amounts payable in connection with administrative or regulatory investigations and proceedings, including regulatory fines and penalties.

4) PCI DSS liability. Generally covers amounts payable in connection with payment card industry demands for assessments, including contractual files and penalties, for alleged noncompliance with PCI Data Security Standards.

5) Media liability. Generally covers third-party liability arising from infringement of copyright or other intellectual property rights and torts such as libel, slander, and defamation, which arise from media-related activities, e.g., broadcasting and advertising.

4. Working with a Broker. Because coverage is changing rapidly, it is important for companies to actively work with their insurance brokers to understand the costs and benefits of evolving coverage and integrate such coverage into an updated Risk Assessment.

B. Capital and Administrative Investment

78 The obligation to limit risks, especially for public companies, is a matter increasingly considered by Boards of Directors. See Mario Chiock, “Cybersecurity and the Board: Where Do We Go
1. **Physical security of hardware.** Making sure the network is protected from physical (i.e. criminal) intrusion or theft.

2. **Network security.** Training personnel and extending resources to ensure the following are up-to-date:
   a. Password protection.
   b. “Access” limited by need.
   c. Access information and authentication.
   d. Firewalls.
   e. Intrusion detection systems.
   f. Antivirus software.

3. **Adopting a risk security framework.** In addition to creating a Risk Assessment and adopting an appropriate Incident Response Plan, a user should strongly consider following the risk security frameworks, and provide third parties assurance that a company is following proper risk remediation procedures. These include:
   a. **ISO 27001.** This has been a primary information security standard since 2005. It includes fourteen groups of controls organized by functional area. A company can obtain certification from the ISO to affirm it has met the standards.
   b. **NIST Cyber Security Framework.** The National Institute of Standards and Technology has created a multi-tiered cyber security framework which includes mapped subcategory and control language for establishing appropriate risk management. The NIST framework focuses on the importance of understanding risk by engaging in a specific process to “identify – detect – respond – and recover” in the event of risks or incidents.\(^7^9\)
   c. **SSAE16.** The SAS 70 was originally created by the American Institute of CPAs. The updated SSAE16 sets a standard control for auditing to insure comprehensive information protection. The SOC 2, TYPE II is


\(^{79}\) There are many different risk management approaches. For example, the Allied Employer Group looks to a five factor risk management wheel: “Identify – Analyze – Action – Monitor – Control.” http://coemployer.com/risk-management/.
the current gold standard for demonstrating comprehensive risk limitation.

d. Updating Standards. Updating is essential because not only is technology of attack and defense in constant flux, but the industry standards are also changing. For example, NIST proposed a new round of updates in January 2017, with comments in April 2017. No organization can ever view its plans as “in stone.”

4. Training. For phishing attacks in particular, training is often the best defense from employees unwisely clicking on links or questionable documents. In any event, users should be trained to immediately notify their IT staff if they have inadvertently clicked on malware.

C. Risk Assessment. This involves looking at your system vulnerabilities, assets, and defenses, assessing risks, and creating a plan to minimize those risks in the most cost effective manner possible. Such a risk assessment, and a plan to prevent an incident, is always a balance between the costs of avoiding the risks and the potential likelihood of an occurrence. It is crucial, when evaluating a potential attack, to understand not only potential threat vectors, but also the information which a bad actor would seek to take and exploit. As with the Incident Response Plan (discussed below), it is crucial that all of the key players, including senior management, participate in supporting a vigorous risk assessment, as well as an appropriate and robust incident response plan. All appropriate stakeholders should be included as part of the risk assessment and incident response plan process.

D. Incident Response Plan. An Incident Response Plan establishes what an organization will do when a cyber incident occurs. (One recent report indicated that only 23% of organizations have a cyber incident response plan applied consistently across the company.)

1. Incorporating the Risk Assessment. A good Incident Response Plan starts with careful consideration of the Risk Assessment (see above) to tailor the incident response to the most likely risks to the business. Indeed, when “testing the plan” (see below paragraph 5) the most likely risks should be used to help practice and respond to the most likely potential incident.

---


82 IBM, More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them, (April 11, 2019).
2. **Establishing a Team.** It is not simply enough to say the incident response team is the IT department. It is crucial that senior managers and, indeed, as appropriate, board level representatives be available to make crucial and timely decisions in response to an incident. (As discussed below, some responses require notification to the public and/or government of a breach or release of PII or PHI.) The team should include not only internal stakeholders, but also outside legal counsel and forensic investigators with expertise in the area to advise the company. Third-party forensic professionals should be ready to supplement internal IT expertise and provide an evaluation and assessment which may be necessary for state and federal authorities.

When a company does not have an IT staff experienced with cyber security responses, it is crucial that an outside company be brought in immediately with the technical expertise to understand the extent of the cyber intrusion and to assist in identification, containment, eradication, and recovery, as well as post-incident response and remediation.\(^{83}\)

3. **Process.** An Incident Response Plan should include processes and procedures for anticipated incidents. The Plan should be supported by specific information that has been used in testing scenarios to quickly and efficiently respond to an incident.

4. **Technology.** Technology should be identified which can permit quick communication of the incident both inside and outside the organization. It is also necessary to ensure there is software in place to track and log what has occurred, to stop any breach, and ultimately lead to eradication. Crucial to Incident Response Plans is not only analytics and statistics concerning the breach, but, where necessary, a business continuation plan, in the event of a catastrophic attack (like a denial of service attack). Part of an Incident Response Plan is having a Business Continuity Management Plan in place which allows the business to continue to operate, even in the face of a dramatic cyber attack.\(^{84}\)

5. **Testing.** An Incident Response Plan is only useful if tested on at least an annual basis. All stakeholders should be involved in the process as much as possible. Using an outside “red team”\(^{85}\) to simulate a cyber adversary can be particularly helpful in identifying weaknesses and problems.\(^{86}\) Moreover, hiring outside consultants to evaluate both the response and weaknesses during

---


\(^{84}\) See generally Ponemon Institute, 2018 Cost of Data Breach Study: Impact of Business Continuity Management (October 2018).

\(^{85}\) See Paul Szoldra, “We Watched a Team of Hackers ‘Fully Compromise’ a Power Company in Less than 24 Hours,” Business Insider (April 28, 2016).

the testing phase can be especially helpful in continuing to refine and improve the Incident Response Plan.

6. Revise and Improve. In the event of an incident, or even as part of regular testing of the Incident Response Plan, the exercise should be viewed as an “ongoing process.” That is, the Incident Response Plan is a “living document” which is steadily updated to reflect changing technology and personnel.

7. Post-Incident Remediation. In the event an incident occurs, it is crucial that the cause of the incident be identified and, wherever possible, the systems in place be modified to prevent a repeat attack in the future. Indeed, many regulatory authorities look to remediation efforts, as well as a risk assessment and incident response plan, as indicia of affirmative efforts to protect private information. The failure to engage in these structured activities tends to result in greater fines and penalties by the regulatory authorities.

VI. RESPONDING TO A BREACH.\textsuperscript{87}

A. Technical/System Phases of an Incident Response.\textsuperscript{88} There is a widely accepted six-step incident response cycle:

1. Preparation. Through a risk assessment and creation of an incident response plan, ideally an organization is prepared for a potential incident and breach.

2. Identification. A breach or incident is identified usually as an anomaly or through detection software. Identifying incidents is one of the key aspects of any defensive system and software.

3. Containment. Once an incident or vulnerability has been identified, the threat must be contained and risk minimized. At the planning stage, risk tolerances will need to be established as part of the risk assessment. When an intrusion has occurred, malware must be contained so the damage is minimized.

4. Eradication. At this stage, internal and external IT professionals seek to restore, update, and, where appropriate, replace sections of the system to eradicate the source of the intrusion.


5. **Recovery.** Once systems are back online, the goal is to return the system to a pre-incident condition and allow normal functioning, while having addressed any vulnerability.

6. **Lessons learned.** This is one of the most important phases in an incident life cycle. The cause and source of the risk is evaluated and new steps are put in place to prevent further intrusions.

B. **Look to Your Incident Response Plan.** Hopefully, the company already has a tested and robust Incident Response Plan in place. The key members of the team (both external and internal) should be immediately notified. Technological processes should be in place to contain, eradicate, and recover from the breach.

C. **Act Immediately to Limit Damage and Mitigate Exposure and Expense.** Having an Incident Response Plan can allow the parties to act quickly to limit and mitigate damages. Containment of data loss is crucial to limit exposure. The time to respond to an incident is seconds, minutes, and hours, not days, weeks, and months.

D. **Determine if Internal or External Attack.** Was the incident the result of outside bad actors, or a malicious current or disgruntled former employee seeking to cause damage or take sensitive data to benefit themselves or harm the company?

E. **Preservation of Evidence.**

1. **Spoliation.** Especially when a company is the victim of an attack by a current or former employee, or a readily identifiable outside party, it is extremely important to preserve evidence to permit forensic examiners to reconstruct how the attack occurred. One of the greatest harms that can occur after an incident is detected is employees or internal IT staff can accidentally engage in spoliation of evidence.

2. **Forensic Copy.** A complete forensic copy should be made of the company’s computer systems after the incident so that a “picture” of the condition of the system at the time the attack was detected is available and, as appropriate, a case against the bad actors can be reconstructed. This is usually done through the creation of a clone forensic copy of the attacked networks, systems, and event logs. Ideally, this should be performed by an outside consultant to maintain appropriate chain of custody and authenticity of the records collected.

3. **Training.** Internal staff should be trained to work with outside experts for the proper handling of electronic data during an incident. This can help lower

---

89 See Robert Boyce and Justin Harvey.
overall costs of the response and protect against future costs and impacts to insurance claims and potential legal compliance and litigation.

4. **Scope of Preservation.** Once upon a time, a “computer” simply meant the large and heavy desktop unit sitting in an employee’s office. Now, most employees access multiple computers in the course of their daily work. Preservation should focus not only on office desktops, but also laptops, tablets, and cloud networks used by employees. One area also overlooked, is that while laptop and desktop computers are certainly important to forensically copy, also the Company’s server (or the portion of it accessed by the employee) must also be forensically copied because for many companies that is where most of the activity actually occurs in the work environment.

F. **Engage Outside Legal Counsel.** Retaining outside counsel can be especially crucial, not only because of the valuable impact of an experienced individual advising a company that has been through a security incident in the past, but, more importantly, attorney-client privilege can protect internal communications from discovery and allow leadership to have a more open and frank discussion about an appropriate response to a cyber security incident. Outside counsel, wherever possible, should also retain outside computer experts in order to maintain attorney-client privilege. Additionally, to the extent law enforcement or government officials need to be notified, legal counsel often plays a pivotal role in facilitating those discussions. Finally and in many ways perhaps most importantly, if management makes decisions on how to proceed in consultation with counsel, management will have the defense of “reliance on the advice of counsel,” which can be very helpful if regulators later second guess management decisions.

G. **Retain an Expert to Provide an Objective and Outside View.** When an incident occurs, even if the IT staff has done everything it should have to limit the possibility of a breach, it is not unusual for these individuals to be either defensive or overwhelmed by the incident. Wherever possible, the attacked company should immediately bring in outside consultants to assist in providing objective information concerning the extent of the cyber intrusion. Indeed, while there is sometimes an instinct to make a full and immediate disclosure to the public and/or government officials, the use of a third party consultant to generate a written report may indicate the data breach was far less intrusive than initially thought and thus a public disclosure may not be warranted. Moreover, outside consultants, in particular those with forensic examination experience, can help pull together information that may be crucial in litigation against wrongdoers especially when it involves former or current employees.

Finally, outside analyses can also include a post-incident analysis to figure out how a company can improve its cyber security posture, thus providing a written record for future regulators, should another breach occur, demonstrating the company’s diligence.

H. **Determine Whether Law Enforcement Needs to be Notified.** The threshold issue is always determining whether law enforcement or government organizations need to be
notified. This turns on fully understanding the nature of the cyber security breach, the data compromised, and the legal obligations of the company to make a disclosure, and/or notify the public, and/or law enforcement or government agencies. Here, consultation with counsel is crucial. Involving law enforcement can be very helpful, especially when criminal level violations have occurred, and law enforcement’s expertise can help assist in responding to the cyber security threat. Moreover, breaches involving PII and PHI may require notification to government officials, and failure to do so can result in significant sanctions.91

I. Determine Whether a Public Announcement is Required.92 Determining whether a “public announcement” needs to be made concerning the breach, whether affected individuals need to be directly notified, or whether law enforcement should be contacted (see above) is often difficult. Outside counsel should play a central role in these discussions, not only to maintain attorney-client privilege (see above), but also to insure that the highest level of corporate leadership is being advised about the serious ramifications of such disclosures.93

J. Determine Whether Notification to an Insurer is Required. The landscape for insurance coverage for cyber security breach is in great flux (see above). However, to the extent an incident occurs and coverage exists, most policies require prompt notifications to insurers.

K. Examine Software and Hardware to Determine Whether the Network is “Clean.” It may seem obvious, but it is essential that the company be assured that both software and hardware are “clean” from any continuing threat. Again, the use of outside consultants to provide third party verification of eradication can provide comfort to senior leadership, shareholders, and government officials that the company is back on track.94

L. Engagement in a Forensic Examination of the Causes of What Occurred. At the end of an incident, after the time and expense of having to deal with an event, companies often want to move on. However, for both legal and practical reasons, it is crucial that a debrief occur to capture lessons learned from handling the incident and to improve on any weaknesses in policy, procedure, or physical and technological security. In the event of a disclosure of PII or PHI, governmental authorities auditing the breach, or examining a subsequent breach, often look to a company’s efforts to insure that a “repeat” does not occur. Good faith efforts by the company to decrease the likelihood of a subsequent incident decrease its potential exposure to liability.

VII. RESPONDING TO SOCIAL MEDIA ATTACKS

Businesses increasingly rely on the internet to attract and retain customers. According to a 2019 Pew Research Center study, 81% of Americans say they go online on a daily basis, and 28% are online “almost constantly.”

This trend makes it critical to maintain a strong online reputation. The risks of failing to do so abound. Gone are the days where disgruntled customers or employees complain to company hotlines or spread rumors through word of mouth. Attacking a company online is easier and more effective. Any person—customer or otherwise—can post a bad Yelp review or damaging Twitter post. More sophisticated attackers can impersonate the company online or hack company accounts. These attacks can reach millions of users before a company ever notices.

A recent survey found that only 57% of respondents considered their organization to very effective in managing reputational risks. These risks are also worrisome for small businesses, especially those unprepared to properly respond to an attack. Even one attack can ruin a company’s reputation and cause loyal customers to go elsewhere.

There are many ways, however, to mitigate the harm suffered by an online attack. These methods can be divided into two stages: (1) proactive measures; and (2) post-attack response measures.

A. Proactive Measures

Harm posed by an attack is much greater if the victim company has no detection or response plans in place. There are steps a company can take to help limit the harm caused by an attack.

1. Manage and Monitor. A company should be aware of and continuously monitor its online presence. This includes several considerations:

   a. Know what is and is not a crisis. A social media crisis is a decisive change from the norm. Some companies are routinely criticized online for company ethics (e.g. Nike, Chick-Fil-A). A true social media crisis is characterized by a markedly different line of criticism.

   b. Set up a listening program. In order to effectively deal with a crisis, a company needs to be aware of its development as fast as possible. This can be achieved by implementing a listening protocol in the

---


organization and leveraging social media listening tools, Google Alerts, and keyword searches.

In addition to identifying its social media presence, a company should create and distribute to employees and executives a social media policy, including guidelines for password use and personal versus company posting. The company may also benefit from appointing an individual or team to routinely check these platforms for any damaging posts. Alternatively (or additionally), a company can purchase “Proactive Social Media Intelligence” to monitor and prevent online social media threats. These programs can be useful, as the faster a company identifies an attack, the better prepared the company will be to respond and minimize harm.

2. **Complaint Procedure.** The company should create clear procedures for responding to an attack. Regardless of the type, a company should be prepared to combat the attack. For example, a company should have a statement directing angry customers to contact the company to help resolve problems. This should be created early and re-used, as these attacks are common. Additionally, a company should create a process for responding to posts containing damaging rumors or misleading information. This process may include appointing a person or team responsible for investigating and responding to the rumor. And, if statements need to be approved by higher level executives, procedures for doing so must also be in place. The faster a company responds to complaints with such statements, the more likely any single attack will be contained. The team makeup will depend on the company type and size, but may include both in-house professionals and external experts.

Last, to help mitigate the effects of an attack, a company should routinely engage with customers online. The more interactive a company is with its customers, the less damaging a single online attack may be. This may also help the company identify an attack quickly.

### B. Combatting an Attack


99 Stacy Collett, *Five Tips for Protecting Your Brand on Social Media*, CSO Online (Oct. 3, 2016), https://www.csoonline.com/article/3126077/social-networking/five-tips-for-protecting-your-brand-on-social-media.html (discussing the need to establish a social media governance program and appoint staff responsible for such governance).

100 One example is the ZeroFox product sold by McAfee. See https://www.mcafee.com/au/resources/solution-briefs/sb-zerofox.pdf.


102 See Hamilton.
1. **Step One: Do Not Act Impulsively or Retaliate.** The initial instinct after discovering a social media attack is to strike back. This can be dangerous. A vengeful response without fully understanding the attack and drafting a proper response can do more harm than good. It can drag the company deep into a dispute that could otherwise be limited. It could also convey the belief that the company does not care about its customers or take responsibility for (alleged) wrongdoing. Instead, take a deep breath, consider available options, and make a proper response.

2. **Step Two: Identify the Nature, Source, and Extent of the Attack.** It is crucial (but not always easy) to identify the attackers. Anonymous posting is very common. If the attacker(s) cannot be identified, a company should at least identify the type of attacker, who may be an angry or dissatisfied:

- Customer
- Competitor
- Employee
- Investor
- Extortionist
- Consumer watchdog

A company should also determine the extent of the attack. This includes searching online for information to identify all platforms on which the attack is taking place or being discussed. This will help identify where and how the company should respond, as a response on social media may differ greatly from a response on a business website. Some common attacks include:

- Posting information or videos on social media websites or apps, including YouTube, Facebook, Twitter, and Snapchat;
- Posting on a consumer review website, such as Yelp, Google Reviews, or Amazon;
- Posting on the company’s commercial website;
- Sending harmful comments to current or potential customers;
- Posting or disclosing harmful information about company executives or employees; or

---


106 See id.
- Hacking a company’s social media accounts and/or establishing fake social media accounts.\(^\text{107}\)

In evaluating the nature and extent of the attack, a company should also consider the attacker’s sophistication, the audience to which the attack is viewable, the likelihood of future attacks, and the potential harm posed to the company.\(^\text{108}\)

3. **Step Three: Evaluate Potential Responses.**

   a. **Contact Media Platform.** Contact the platform provider directly or utilize the provider’s reporting mechanisms. For example, Yelp allows reporting and removal of fake or defamatory reviews, and Twitter and Facebook allow reporting and blocking of harmful or abusive users.\(^\text{109}\) If the damage can be contained using these procedures, this should be the first option.

   b. **Contact the Known Attacker Directly.**\(^\text{110}\) A disgruntled customer or employee may respond more positively if contacted personally.\(^\text{111}\) Research has found that approximately 1/3 of customers receiving a personal response to their negative review deleted the negative review and/or posted a positive review.

   c. **Reaching Out to Unknown Attacker.**\(^\text{112}\) By posting a polite message asking the attacker to contact the company directly, a company may cure the underlying problem that triggered the online attack, and will show other viewers that the company is attentive to its customers.\(^\text{113}\)

   d. **Issue Public Statement.** The more individuals publicly expressing concern, the more appropriate a public statement becomes. To the

---


\(^{108}\) See id.; see also VORYS.


\(^{111}\) See Baer and Teague (Adopting the “Hug Your Haters” response rule to give an agitator two responses, but no more).

\(^{112}\) Id.

greatest extent possible, a company should carefully draft its response to frame the issues positively. The message should focus on affirmative steps taken to remedy a legitimate concern raised by an attacker.

4. **Step Four: Legal Action.** A final option is to pursue legal action. This may include hiring an attorney to craft and send a cease and desist letter. It may also include filing a defamation claim. Defamation claims, however, are notoriously difficult to prove. Generally speaking, to prevail on a defamation claim, a private plaintiff must prove harm resulting from a publisher negligently making a false statement to an unprivileged third party. Each state may have different requirements to prove defamation.

The growing number and variety of social media platforms certainly increases the number of harmful statements communicated to third parties. But, this increase in statements does not necessarily ease a victim’s burden in proving defamation. This is because, first, social media may blur the line between false statements and opinions. Because opinions often trigger First Amendment protection, investigating the statement and its context is critical.

Another difficulty in proving defamation in the digital era is identifying the publisher. As discussed above, social media often brings an element of anonymity (false names, anonymous postings, etc.) that makes it difficult to discover the potential attacker. This is further complicated by the fact that social media providers typically have strict user privacy protections, which can make it difficult to work with an online provider to discover or remedy a user’s defamatory statements. Relatedly, a company would be wise to preserve all evidence of the defamatory statement in case it is subsequently removed.

While some believe internet platforms or website hosts should be liable for defamation, these claims are largely precluded by the Communications

---

114 See Kim Harrison, How to Respond to a Social Media Attack, https://cuttingedgepr.com/blog/respond-social-media-attack/


116 VORYS, note 9, at p. 15.

117 See RESTATEMENT (SECOND) OF TORTS § 558.


119 Id.

120 See id.; see, e.g., Facebook, Law Enforcement & Third-Party Matters, https://www.facebook.com/help/473784375984502 (noting that the Stored Communications Act “does not allow private parties to obtain the content of communications . . . using subpoenas”).
Decency Act. Thus, claims must be initiated against the attackers themselves.

Defamation claims are not impossible to prove, however, and may lead to large recoveries. For example, in 2013, the Miss Universe Organization was awarded five million dollars in damages following defamatory statements made online and on television by a former contestant. Additionally, according to a Washington Post article, “an Anaheim, Calif., technology company won a $1.6 million judgment against a blogger who had accused the company of stealing money from business associates. And in 2006, a Florida woman won a $11.3 million judgment after a Louisiana woman called her a ‘crook’ and a ‘con artist' in an Internet forum.” In 2017, Disney (which owns ABC) agreed to pay a beef products company $177 million to settle a defamation claim after ABC reported that the beef company was using an unsafe “pink slime” product in its beef.

C. Conclusion.

Time and money are well spent monitoring social media and having a team in place to respond quickly to an attack. Rapid and effective action can mean the difference between a minor annoyance and a major PR disaster.

VIII. 10+ TIPS TO STAYING SAFE.

1. Invest in active protective software. Protect against viruses, malware, and other malicious code. Make sure each of your computers is equipped with antivirus software and antispyware and update them regularly. Such software is readily available online from a variety of vendors. All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install updates automatically.

2. Secure your networks.

---

125 See Peter Gasca, How to Fire Back at an Angry Customer on Social Media (Sept. 11, 2014), https://www.entrepreneur.com/article/237196.
33

a. **Wi-Fi.** Safeguard your internet connection by using a firewall and encrypting information. Two main encryption protocols are Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Wherever possible, use WPA3 which presents the strongest level of encryption against hacking. Make sure Wi-Fi networks are secure and hidden. To hide a Wi-Fi network, set up the wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

b. **Router.** Your router redirects traffic between your local network and the internet. Change your default name, reset your passwords, eliminate remote management features and set up yourself as the new administrator. Whenever updates are available, make sure you perform them on your router.

3. **Protect personal information.**

a. **Policies.** Establish security practices and policies to protect sensitive information. This includes social security numbers, credit cards, bank information, and other highly sensitive business and personal information. Establish policies on how employees should handle and protect personally identifiable information and other sensitive data. Clearly outline the consequences of violating cyber security policies.

b. **Transmission.** Personal and other sensitive information like banking and credit card data should only be provided over encrypted secure servers. Look for sites with “https” at the beginning of the website address.

4. **Employee training and accountability.**

a. Educate employees about cyber threats and hold them accountable.

b. Educate employees to avoid phishing attacks.

c. Prohibit employees from inserting USB drives into any network computers without first having them fully checked for malware.

d. Employees should be informed about how to post online in a way that does not reveal any trade secrets to the public or competing businesses.

5. **Strong passwords.**

a. **Passwords.** Require employees to use strong passwords and to change them often – at least 10 characters that are unpredictable. They do not need to be “random,” but do need to be difficult to identify. Check with
vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication.\textsuperscript{127}

b. \textbf{Two-Factor Authentication.} This requires the password and additional information or a step to complete authentication. This often involves a code being sent to a phone or an additional e-mail address to authenticate computer access.

6. \textbf{Employ best practices on payment cards.} Work with banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used. Consider additional security obligations related to agreements with banks or processors. Isolate payment systems from other, less secure programs and do not use the same computer to process payments or surf the internet.

7. \textbf{Backup data.} 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 on the cloud.

8. \textbf{Control physical access to computers and network components.} 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. \textbf{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.\textsuperscript{128} Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the device is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

10. \textbf{Website protection.} Protect all pages on your public-facing websites, not just the checkout and sign-up pages.


\textsuperscript{128} According to one study, security professionals rank mobile devices as the highest level of cyber security concerns, ahead of both data cloud-related issues and user misbehavior. See Cisco Systems, \textit{2017 Annual Cybersecurity Report}, p. 10 (2017).
STEPHEN E. YOCH
ATTORNEY

Direct: (612) 373-8559
Email: syoch@felhaber.com

ADMINISTRATIVE ASSISTANT
Deb Murphy | (612) 373-8513

PRACTICES
Business & Commercial Litigation, Business Law and Transactions, Civil Litigation, Computer and Technology Law, Construction Law, Mergers & Acquisitions, Outside General Counsel, Real Estate

INDUSTRIES
Construction, Manufacturing, Real Estate Development, Technology

AWARDS
"AV Preeminent" Rating by Martindale Hubbell, North Star Lawyer, Super Lawyers*

OVERVIEW
Steve Yoch enjoys helping clients avoid and solve problems. His extensive business, transactional, and litigation experience allows him to assist clients in evaluating all the alternatives when facing legal challenges. Most importantly, Steve values the long-term relationships he develops with his clients.

Steve is a member of the Felhaber Larson Board of Directors and is on the Management Committee.

Steve Yoch on Linkedin
Steve Yoch, Author, on Facebook

EXPERTISE & CREDENTIALS

Practice Areas
- Business Organizations and Transactional

https://www.felhaber.com/people/stephen-e-yoch/
- General Corporate Law
- Business Acquisition and Sale
- Commercial Contracts
- Real Estate Law
  - Construction Law
  - Land Acquisition and Sale
  - Lease Negotiations
  - Landlord Tenant Disputes
- Civil/Commercial Litigation
- Cyber Security and Response

Representative Work
- Steve provides general corporate advice to a variety of businesses, including manufacturing, real estate, construction and service companies. He has expertise in cyber security prevention and response.
- His transactional experience includes business acquisition and sale, construction agreements, land acquisition and sale, business contracts, and lease negotiation.
- His litigation experience includes contract, shareholder, construction, landlord/tenant, non-competition, probate and copyright claims.

Professional Certifications, Awards and Designations
- Named in Super Lawyers®, 2003-2019
- Rated “AV Preeminent” (highest rating) by Martindale Hubbell Legal Directory
- Cybersecurity and Privacy Law Certificate, Mitchell Hamline School of Law
- Certified Distance Education Instructor, IDECC & Arelló

Bar Admissions
- Wisconsin, 2003
- Minnesota, 1990

Education
- J.D., University of Minnesota, cum laude, 1990
- B.A., Boston College, cum laude and Scholar of the College, 1987

ARTICLES & PRESENTATIONS

Articles
Written over 50 articles on legal topics. Examples include:
- The "Minnesota Real Estate Deskbook", published by Minnesota CLE (Co-editor)

https://www.felhaber.com/people/stephen-e-yoch/
“All Breaches Are Not Created Equal - Understanding Default and Breach”
“Before You Cash That Check...”
“Can You be Bound by an Arbitration Agreement You Didn’t Sign?”
“Email: When ‘You’ve Got Mail’ Means ‘You’ve Got a Deal!’”
“Force Majeure - A Clause for Our Times”
“Getting Paid in the Event of a General Contractor Bankruptcy”
“Hey! They stole my plans! Architectural Copyright in Minnesota”
“How Do You Sign a Contract?”
“Indemnification Agreements - You Want Me to Pay for What?”
“It's Not Easy Being Green: Legal Pitfalls of Green Construction”
“Key Warranty Issues”
“Legal Implications of Building Information Modeling”
“Legally Running a Company (or Else)”
“Limitation on Damages Clauses – We Made a BIG Mistake!”
“Real Estate Deskbook — Property Tax Considerations”
“Right to Audit Provisions - Trust ButVerify”
“Selecting an Entity and Controlling It”
“Summary Guide to Construction Claims”
“The Personal Side to Personal Guarantees”
“The Tides are Turning - Weathering the Storm of Uncertain Financing”
“Warranties 101”

Presentations
Presented and taught over 50 seminars and classes to lawyers and industry groups. Examples include:

“What You Need to Know About Cyber Security & Social Media Attacks”
“Essentials in Protecting Yourself from Personal Liability Claims”
“I Want Out of the Deal Minnesota’s Statutory Cancellation”
“Leasing in Troubled Times: Negotiating and Enforcing Commercial Leases in a Distressed Market”
“Modifications of Owners Plans – Cost or Opportunity?”
“Mortgage Fraud Prosecutions in Minnesota”
“Negotiating and Completing Commercial Real Estate Closings”
“Summary Guide to Construction Claims”
“The Eye of the Storm: Preparing for the Next Cyber Security Incident”
“Three Stupid Legal Mistakes in Leases”
“Work-Outs, Debt Restructuring, and Other Ways to Stay Financially Fit”
“You Can’t Do That! Restraints on Trade: Non-competes, Confidentiality and Other Agreements”

MAKING A DIFFERENCE

BATC Foundation – Volunteer Attorney
Minnesota CLE Real Estate Institute Planning Committee
Board of Trustees, Mounds View School Educational Foundation
Southern Minnesota Regional Legal Services (SMRLS), Volunteer Attorney for 25+ years. Steve talks about how he began working with SMRLS:

https://www.felhaber.com/people/stephen-e-yoch/