CLM and The Retail, Restaurant & Hospitality Community Advisory Board
February 8, 2018
Renaissance Dallas Hotel

# Cyber Security Bingo – Don't Get a Blackout!

**Cyber Security Bingo – Don't Get a Blackout!**

**Cyber Attacks**

The most significant trend in 2016 was the emergence of ransomware as a key cyber attack weapon. No industry escaped ransomware attacks. The costs of handling a ransomware attack will typically eclipse the costs of the ransom demand. Additional factors that can increase costs significantly include business interruption and the need to restore lost data post attack. In a ransomware attack, the perpetrator releases a virus to systematically encrypt files, then demands payment of a ransom, usually in a crypto-currency such as Bitcoin, in exchange for the key to decrypt the data. A new form of attack exploits the remote desktop protocol (RDP) functionality that is a part of Windows systems. RDP allows a user to establish a connection to a remote computer and is often configured for legitimate purposes. But when users have weak passwords or an organization doesn't monitor service accounts, attackers can use brute force attacks to gain access to accounts with administrator privileges, giving them wide access to the network. Phishing, hacking, and/or malware represent 43% of all cyber incidents with 23% of that total being ransomware.

Employee actions and/or mistakes represent 32% of cyber incidents. There are many ways insiders, malicious or nosy employees, can wreak havoc on an organization – from feeding data to an identity theft ring for profit, to peeking at a celebrity patient's medical records. Unauthorized access to data by insiders can lead to costly and time consuming audits and forensic expenses to determine the extent of a breach, even before a full response can be marshalled.

Lost or stolen devices or records account for 18% of cyber incidents. These breaches happen simply but they can involve a complex response requiring legal, forensics, notification, call center and credit monitoring assistance. Responding to a stolen unencrypted portable device incident can cost hundreds of thousands of dollars. Regulators tend to come down hard on organizations that do not take the relatively simple and effective precaution of full disk encryption on the device.

Retail, Restaurant and Hospitality providers present extremely tempting targets for identity thieves. Publicly available wireless networks, physical point of sale devices within restaurants and bars, and a multitude of employees with access to guest information all increase the risk. Smaller, independent organizations may be challenged to allocate sufficient resources to network security in a world in which hacking and malware threats evolve very rapidly. For larger franchise operations the biggest risk may be

interconnectivity: if franchisees and the franchisor share a single hospitality management system, one small mistake or vulnerability can lead to a breach that results in significant and lasting reputational damage.

Retail, Restaurant and Hospitality commerce without credit and debit card payments has become virtually unimaginable. Whether at the point-of-sale, online, or through a call center, the hospitality industry processes a staggering amount of credit card transactions. A breach of credit card information, which the card brands frequently detect before the organization even suspects any foul play, can result in fines, penalties, mandated computer forensic costs, legal fees, and worst of all, the inability to process payments.

The publicity and customer dissatisfaction that surround a cyber breach have incentivized a wave of class action complaints against retail, restaurant and hospitality companies big and small. Enterprising plaintiffs' lawyers relying on a variety of privacy laws have filed complaints seeking billions of dollars in damages. The specter of such annihilating damages, and the sizeable costs of litigation, often push organizations to settle even in the absence of any clear harm to the plaintiffs.

State and federal regulators have made one point fundamentally clear: a significant breach of customer information will result in monetary penalties, onerous corrective action plans, and on-going audits. Whether from the Federal Trade Commission or state attorneys general, the regulatory landscape for the retail, restaurant or hospitality industry carries an immense amount of risk.

Typical Incident Response Timeline – From Detection, Through Containment, To Notification

61 days from occurrence to discovery

8 days from discovery to containment

40 days from engagement of forensics until forensics investigation complete

41 days from discovery to notification

**Prevention is ideal, detection is a must**

Most organizations are compromised for an average of 130-200 days before they realize they have an issue. Many organizations have a false sense of security that leads to vulnerability. On top of that there is no "one size fits all" easy solution to the problem of cyber attacks. A roadmap for successful cyber attack prevention looks like this:

*Determine your risk appetite by doing audits, continuously scan you system, perform vulnerability assessments, and execute penetration testing.* See below for assessments with different purposes:

| Assessment Type | Security Audit | Vulnerability Assessment | Penetration Test | Social Engineering |
|---|---|---|---|---|
| Purpose | Evaluation of how various security processes are designed and implemented for a particular system, environment, or organization. Lays out a plan for evaluation and areas of focus. | Comprehensive identification and evaluation of known vulnerabilities in the computing environment typically involving a combination of the use of scanning tools, network diagram reviews, and reviews of device configurations. | Seeking to mimic the actions of a hacker – looking for any way to circumvent security controls to gain unauthorized access, typically without being detected. | Performing phishing, vishing and other techniques often used by hackers to deceive users into compromising their own security. |
| What is Accomplished? | Recommendations for enhancements to fix security management processes. | Identification of known technical vulnerabilities in networks, operating systems, databases and applications. Tests the adequacy of the vulnerability management process. | Narrow identification of known vulnerabilities based on the techniques used by the pen tester. Determine the exploitability of identified known vulnerabilities. Tests effectiveness of incident identification, response procedures. | Tests the effectiveness of the organization's security awareness training program. Social engineering tactics are often used to deceive users into divulging their logon credentials or to get a user to download malware. May test effectiveness of incident identification, response procedures. |
| What is Not Accomplished? | Typically not able to assess effectiveness of incident identification or response procedures. May not get good visibility into technical system vulnerabilities. | Root cause of why known vulnerabilities exist in the environment. Unsure exactly how exploitable known vulnerabilities are. Unable to assess effectiveness of incident identification or response procedures. Won't catch 0 day vulnerabilities. | Typically don't have a comprehensive understanding of all known vulnerabilities. Will not involve 0 day vulnerabilities. | Doesn't comprehensively evaluate the design and effectiveness of security management processes and doesn't identify technical vulnerabilities. |

*Use anti-virus, anti-malware, patching updating, and perimeter security*

*Develop incident response plans – create, implement and train*

*Develop business continuity plans that are tested for effectiveness in the event that it needs to be implemented*

*Outmaneuver your adversary – are you currently breached and just don't know it?*

**Legal Environment**

Domestically 48 states, D.C. and all U.S. territories have breach notification laws. These laws basically require notification of a "breach of the security of the system" to individuals whose personal information was accessed or acquire by an unauthorized person. These laws are frequently amended to:

Expand the definition of personal information

Set forth a specific time deadline for notification

Require notification to the Attorney General

Clarify or add exception for encrypted data or no reasonable likelihood or harm exception

*Payment Card Industry Data Security Standards*

Under this rules, a business may be required to obtain and pay for a computer forensic audit. If they are suspected to be the source of a breach event, a business may be subject to fines, penalties and loss assessments should they be the source of the breach. PCI loss exposures are based on a contractual liability rather than tort law. The most important contractual requirement is to adhere to the PCI DSS. There are the rules that require merchant banks, processors and merchants to maintain specific security requirement to protect card data from being stolen. The PCI DSS are complex. They cover 12 different areas and have over 200 specific requirement. Depending on the number of card transactions that they process each year, merchants must certify compliance with PCI DSS by completing a Self Assessment Questionnaire (SAQ) or by paying an outside auditor to complete a Report on Compliance (ROC). Importantly, the responsibility to remain in compliance with the PCI DSS is continuous. Merchants must be careful to remain in compliance at all times. Merchants also generally agree to the following:

> Forensic Audits: if suspected to be the source of a breach the merchant is required to obtain a forensic audit of their computer system by a computer security expert approved by the card brands. Such forensic investigation can cost well over $100,000.
>
> Fines and Penalties: if found to be out of compliance with PCI DSS, merchants may be subject to fines and penalties. These are between $5,000 and $50,000 each month the merchant is out of compliance.
>
> Loss assessments: If the merchant is found to be out of compliance with PCI DSS and cards were at a risk of being breached, they may be subject to assessments to compensate issuing banks for the cost of issuing replacement cards to consumers as well as the cost of fraudulent charges paid to merchants but which cannot be collected from consumers.

*European Union's General Data Protection Regulation (GDPR)*

The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation will take effect after a two year transition period and does not require any enabling legislation to be passed by the government, which means it will be in force January 2018. The GDPR not only applies to organizations located within the EU but it will also apply to any organizations outside the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data or data subjects residing in the EU, regardless of the company's location. For example, a US domiciled online retailer, with no corporate presence in the EU, markets its products globally and allows website visitors to view product prices denominated in Euros. This organization may very well be subject to the obligations within the GDPR with respect to those European citizens visiting its website. The regulation sets out a single data breach notification requirement designed to be applicable across the EU. It requires notice to DPA within 72 hours of discovery as well as notice to individuals without delay if the breach is likely to result in high risk to individuals. Organizations can be fined up to 4% of annual global revenues for breaching GDPR or $10 million Euros. This is the maximum fine that can be imposed for the most serious infringements. There is a tiered approach to fines.

**Insurance**

*Cyber Liability* is largely data breach insurance. It focuses on emerging risks arising from information technology that are outside the scope of traditional insurance policies. Tradition insurance is generally focused on issues of physical damage and bodily harm. The core components of a cyber liability policy are designed to help companies deal with specific legal obligations and liabilities associated with a loss, theft or unauthorized disclosure of confidential information.

*Legal liability coverage* is defense costs and indemnification for amounts that the insured is required to pay as damages because of a data breach. There are three key third party legal liability coverages provided for data breach events. Coverage for claims seeking damages – most often class action claims. Coverage for legal representation for a regulatory investigation probing a data breach event as well as for fines resulting from such investigations. And lastly, coverage for amounts that the insured is contractually liability to pay as fines and loss assessments to payment card issuers under a merchant services agreement.

*Breach response* costs are expenses incurred to investigate an actual or suspected breach event and to comply with legal obligations arising from such event. These items are focused on helping an insured to determine if they have a legal obligation to notify consumers of a data breach event and funding the cost of such an obligation. Coverage typically includes costs to investigate the incident, obtain counsel, notify consumers, and crisis management expenses. Credit monitoring is often offered to consumers and this is also covered.

Some type of *media liability* is normally offered on Cyber policies to address gaps in a General Liability policy. The coverage may be internet media only or possibly multimedia.

*Cyber Extortion coverage* will indemnify an insured for amounts paid under duress arising from threats to damage or release data from the insured's computing system or to disable or interrupt the normal operations of the insured's computer system. The most common extortion are ransomware attacks (previously discussed). Denial of service attacks are also common and used against online merchants during peak periods. Under this scheme, the bad actor will flood the victim's computer system with a stream of data. The victim's system will be overwhelmed and will be shut down. The bad actor will continue this attack until the victim agrees to pay a ransom.

*First Party coverages* are also available for data protection and business interruption. Data protection pays the insured's costs to recreate or restore data corrupted or deleted due to a failure of computer security. Business interruption coverage is for the insured's loss or income or extra expenses. Most forms are triggered by a failure of computer security. Some can be triggered by a data breach event. Sometimes loss due to a hardware or software failure within the insured's computer system is also covered (systems failure coverage).

*Emerging Coverages*

> *Reputational Damage* will indemnify an insured for a reputational damage loss incurred during a network event restoration period. Reputational damages are the loss of net income due to termination of your service contract by one of your clients and/or reduction in the value of your business and brands where such loss arises directly from a network event.

*Social engineering coverage* will indemnify an insured for a loss when an employee has been tricked into sending money or securities to a bad actor by virtue of a fraudulent instruction intended to mislead the employee through the misrepresentation of a material fact that is relied upon in good faith by the employee. A very common scheme is for the bad actor to impersonate a vendor and request the insured to change the vendor's wire transfer account number.

*Dependent business interruption coverage* provides insurance for an insured's loss of income and extra business expenses resulting from a covered loss to a supplier or another business that an insured depends upon to maintain normal business operations. Dependent business may be limited to providers of information technology or computer services. Broader coverage would extend to any third party entity that provides necessary products or services to the insured.

*Contingent business interruption* extends coverage to a loss of income or extra business expenses incurred due to an otherwise covered loss to a customer of the insured.

*Vendors*

A typical cyber liability policy provides the insured's with vendors who provide extremely important services to the insureds. Privacy counsel and forensic experts are provided to help clients establish what data has been compromised, assess responsibility, and issue appropriate notifications. Mailing and Call Center vendors provide timely notification to affected individuals. Credit or identity monitoring vendors provide affected individuals with those services. Lastly public relations and crisis management services are provided to help safeguard reputations. An example of services provided during a ransomware attack would be the availability of legal counsel and external forensics support. Operating hand in hand with legal counsel 9under the attorney-client privilege and work product doctrines) forensics experts help determine how the ransomware entered the system and whether it had additional functionality, such as the ability to exfiltrate data. If data was compromised, legal counsel advises on notification obligations.