2018 CLM New York Conference
December 12, 2018
New York, NY

NARRATIVE

Presentation Title: A Best Practice Approach for Protecting PII & Mitigating Security Risks in 2019

In today's information economy, companies across every industry are faced with the challenge of securing information assets. In fact, with cyber security threats on the rise, insurance claims departments, in-house counsels, law firms and their third-party partners who frequently exchange documents containing Personally Identifiable Information (PII), all are becoming more vulnerable.

Corporate Focus

The first area that we will discuss, is the importance of corporate responsibility and leadership around data security.

Security Blossoms in the Boardroom

Sadly, security breaches will continue to be a regular occurrence in 2019 and organizations will struggle to deal with them. New security challenges will abound and these will grab attention in the boardroom. Senior management is increasingly focusing on security issues and recognizing them as a core business risk, rather than the responsibility of the IT department alone. The coming year will see further commitment from the boardroom to ensure that organizations are protected.

Company Culture

- In order for an organization to truly embrace compliance and data security as part of their culture, it must begin from the top leadership in the organization.
- It is important to not only educate your teams on the subject, but you should also offer on-going training to all levels of your staff.

New Privacy Policies

A privacy policy can be one of the most important documents on a company's website. It details an organization's views and procedures on the information collected from visitors. Although a privacy policy is technically a legal document, great effort should be made to craft a document that is both accurate and easy to understand, obscuring hidden clauses in reams of text is not acceptable.

GDPR—Have businesses missed the point?

GDPR replaces the EU Data Protection Directive (DPD) adopted in 1995 and is intended to establish one single set of data protection and privacy rules across Europe. If your company collects data concerning any EU citizen, GDPR applies to you, irrespective of where you are located. The crux of GDPR is that it gives control back to EU residents over their personal data being held by companies. They have a right to know why the personal data is being processed, have access to it and have the ability to have it erased.

A key part of the regulation requires consent to be given by the individual whose personal data is held. Consent means "any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed."

Furthermore, the company or organization must be able to show how and when consent was obtained. This consent does not need to be explicitly given; it can be implied by the person's relationship with the company. However, the data obtained must be for specific, explicit and for legitimate purposes.

The arrival of GDPR in May 2018 was, of course, a big story. However, many organizations are missing the main point about GDPR. It is about identifying, protecting and managing PII – any information that could potentially identify a specific individual. This will become more important in 2019 and there will be considerable focus on identifying, securing and, where required, deleting PII held on networks.

Unfortunately, GDPR will give a great opportunity to criminals, hackers, disgruntled staff and anyone who might want to do organization harm. They simply have to ask you to identify what data you hold on them, ask for it to be erased, and ask for proof that it has been done. If you can't comply, they can threaten to go public – exposing you to the risk of huge fines – unless you pay them money. Watch out for this one!

<u>Cyber Crimes</u>

IoT – A security time-bomb

IoT (Internet of Things) is a rapidly growing phenomenon which will accelerate in 2019, as both consumers and businesses opt for the convenience and benefits that IoT brings. However, manufacturers are not yet routinely building security into IoT devices and 2019 will see further problems generated through the use of insecure IoT. IoT is a major threat and possibly the biggest threat to businesses in the coming years.

Unfortunately, it is not easy, and in some cases impossible, to bolt on security as an afterthought with IoT, and many organizations will find it challenging to deal with the consequences of such breaches. As IoT cascades through organizations' infrastructures, it is likely to become the ultimate Trojan horse.

Ransomware has not gone away

Too much money is being made from ransomware for it to disappear – it won't. The U.S. Department of Justice (DOJ) recently described ransomware as a new business model for cybercrime, and a global phenomenon. Global ransomware damage costs for 2017 exceeded $5 billion, with the average amount paid in ransom among office workers around $1400.

Cyber Security Ventures: Companies can help prevent ransomware by tracking everything coming in and out of the network and running anti-virus solutions with anti- ransomware protection. And, of course, you should do regular backups to a structured plan, based around your own business requirements – and make sure you test the plans.

Social Engineering Schemes

In today's business climate, social engineering schemes are ever more prevalent – as hackers continue to look for vulnerable businesses to prey upon in an effort to fraudulently wire transfer large sums of money from an innocent internal employee. Some industries are much more prone to such attacks than others – particularly those that handle client funds, including real estate, accounting, and investment advisors. While many social engineering schemes are effectuated through malware attacks and spear phishing campaigns, others are completed through victims of pretexting, baiting, Quid Pro Quo or tailgating.

Companies who handle large amounts of client monies should have regular, rigorous and continuous training efforts of employees who are in positions to transfer funds. Further, such companies should assess that they have sufficient risk transfer programs in place, including sufficient commercial crime and/or cyber insurance to ensure that such risks are covered in the event a social engineering scheme takes place.

The Insider Threat

Historically, insider threats have been underestimated, yet they were still a primary cause of security incidents in 2018. The causes may be malicious actions by staff or simply poor staff cyber-hygiene – i.e. staff not using the appropriate behavior required to ensure online "health."

In 2019, there will be growth in cyber education, coupled with more testing, measuring and monitoring of staff behavior. This increasingly involves training and automated testing, such as simulated phishing and social engineering attacks.

More from the Shadow Brokers

The Shadow Brokers, a hacker group which stole hacking tools from the American National Security Agency (NSA), created havoc in 2017 with the Wannacry ransomware episode. The group has already stated that it will soon release newer NSA hacking tools, with targets that might include vulnerabilities in Windows 10.

There will certainly be further episodes from them in 2019, so patch management, security and regular backups will be more crucial than ever. A major target of these hackers is the data that organizations hold, including PII (Personally Identifiable Information) and corporate data, so protecting the data 'crown jewels' inside the network will become ever more crucial.

DDoS on the rise

It is now possible for anyone to 'rent' a DDoS attack on the internet. For as little as US$ 5, you can actually pay someone to do the attack for you! This is just one of the reasons DDoS threats will continue to escalate in 2019, alongside the cost of dealing with them.

The dangers of DDoS for smaller companies are that it will leave them unable to do business. For larger organizations, DDoS attacks can overwhelm systems. DDoS is significantly under-reported, as no-one wants to admit they have been under attack!

Paper Records are a Threat Too

According to a study published in The American Journal of Managed Care, Paper and film records account for the most common location of data breaches in hospitals.

During the 2009 to 2016 study, researchers found that hospitals comprised roughly one-third of all healthcare breaches. Paper- and film-based records, rather than electronic records, comprised 65% of hospital data breaches. In fact, network servers were the least common location of breached data, although their breaches affected the greatest number of patients.

Hospitals need to hold themselves to conduct routine audits to allow them to see their vulnerabilities before a breach occurs. Additionally, information security systems should be implemented concurrently with health information technologies. Improving access control and prioritizing patient privacy will be important steps in minimizing future breaches.

Security Best Practices

Time to Ditch Those Simple Passwords

In 2019, simple passwords will be even more highlighted as an insecure 'secure' method of access. Once a password is compromised, then all other sites with that same user password are also vulnerable. As staff often uses the same passwords for business as they use personally, businesses are left vulnerable. While complex passwords do have a superficial attraction, there are many challenges around that approach and multi-factor authentication is a vastly superior method of access.

Never Send Unencrypted Emails Containing PHI

Everything sent in an email, from the attachments to the text, goes on a dangerous journey. Its path is filled with many traps that cybercriminals can use to steal information. The HIPAA Security Rule requires us to take a risk management approach to the security of protected health information. It also sets out a bunch of standards we need to implement as part of our risk management plans (that "Transmissions Security" standard was one of them.)

{Standard: Transmission Security
Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. *US Department of Health and Human Services, 2005}*

To protect the content of an email it should be encrypted. This way, even if someone is able to access the email itself, the content cannot be read.

The journey that an email takes is not as straightforward as one might think. It isn't a simple matter of going from A to B, but rather the emails pass through different routes which put them at risk of attack from cybercriminals:

1. The email sent from your device to your company's server. Larger companies generally make sure that this is a safe route and look after it.
2. The email needs to pass through different serves until it reaches its destination. This part of the journey is the most dangerous as the email can be intercepted at any time, especially if the server used by the receiver is not protected correctly. The worst thing about this stage is that users are completely blind – **there is no way of knowing how secure the connection is between the two servers.** The only way to be sure is to encrypt your messages.
3. Not only is the email going between two servers, but the email still has to travel to the computer or the mobile device. This stage can also be complicated and, furthermore, once it arrives at the other device it can still be under threat. Computers are always at risk if the correct security procedures aren't followed.

With so many different ways to steal information from emails, it is vital to protect the content and attachments that you send or do not send them via email.

Cloud Insecurity – It's Up To You

Problems with cloud insecurity will continue to grow in 2019 as users put more and more data on the cloud, without, in many cases, properly working out how to secure it. It is not the cloud providers' responsibility to secure the information – it is down to the user.

With the introduction of GDPR in 2019, it will be even more important to ensure that PII stored in the cloud is properly protected. Failure to do so could bring serious financial consequences.