Privcap/
CONVERSATIONS

Q4 2015

Preparedness Is Key In Cybersecurity

"There are many insurance carriers and brokers that are now dealing with cyber liability policies."

– Andy Obuchowski, RSM US LLP

WITH EXPERT COMMENTARY FROM: RSM US LLP

SPONSORED BY RSM

Click to watch video
➜ Preparedness is Key in Cybersecurity

Preparedness is Key in Cybersecurity

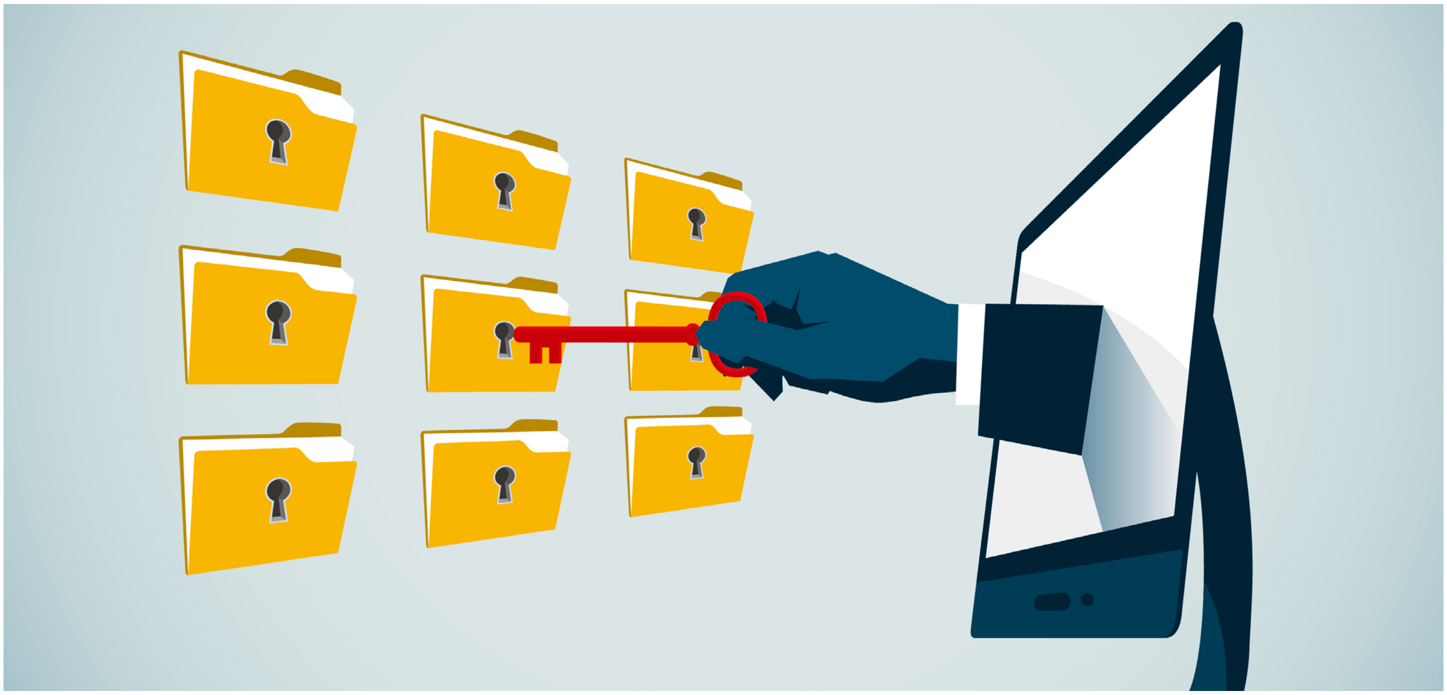
Staying ahead of cyber-threats with information on the latest hacking tools is one way to avoid a data breach

Andy Obuchowski
Director of Security and Privacy,
RSM US LLP

➜ BIO

Obuchowski is the national leader and supports global operations for cybercrime and data breach investigations, digital forensics, and incident response services within the security and privacy consulting group. Obuchowski possesses more than 20 years of experience, including 12 years of law enforcement investigations, instruction at numerous police academies, and long-time memberships in several computer and financial crime task forces. He is also currently an adjunct professor of criminal justice at Anna Maria College in Massachusetts, where he developed and teaches graduate and undergraduate programs in information security, digital forensics, and cybercrime investigations.

CONTINUES ON NEXT PAGE



Privcap: How do you define cyberforensics?

Andy Obuchowski, RSM: Cyberforensics is a broad term, but to keep it simple, it's a scientific process of collecting and analyzing electronic media or information because of a past event.

For example, it could be the collection of information from computer systems, email accounts, network file shares, and third-party applications. We're looking for evidence of information that was transferred from a computer either by theft or some other type of malicious intent.

Who are current major targets for cybercrime?

Obuchowski: Healthcare is a major target because healthcare information is worth more on the black market than an individual's credit card or personal identity. Instead of using a stolen credit card number in order to obtain some type of immediate financial gain, an identity thief will steal an individual's healthcare information to commit health identity theft. Instead of assuming a person's identity based upon a name and date of birth, they're assuming a person's identity based on his or her healthcare information, and it can be used for fraudulent claims or fraudulent treatments.

Who is purchasing this information?

Obuchowski: Anybody who knows where it is on the black market. Personal information such as a name, date of birth, or a credit card number on the black market may only go for a few dollars per record. However, their healthcare record could go for somewhere between $300 or $400 per instance.

What do you find is the biggest target besides healthcare?

Obuchowski: There tends to be a lot of focus on personal identifying information such as name, dates of birth, bank account records, credit card information, or healthcare records. But when it comes to a company a big target is intellectual property (IP).

If a company is going to build a new latest and greatest product, why not try to steal that intellectual property, ship that information overseas where you can then essentially manufacture that product for a fraction of the cost and then beat them to market? Having any type of legal recourse is very challenging due to different regulations and laws in different jurisdictions.

Is there insurance for cyber theft?

Obuchowski: There are a lot of insurance carriers and brokers out there that are now offering cyber-liability policies. These policies deal with the insuring of an incident, and generally it's meant to be more of the digitally related kind like computer intrusion,

> “There are a lot of insurance carriers and brokers out there that now are dealing with cyber liability policies.”
>
> –Andy Obuchowski, RSM US LLP

CONTINUES ON NEXT PAGE

otherwise known as hacking. So there are policies to help cover the costs when dealing with the theft and the investigation of information.

However, it becomes a challenge when you're looking at the theft of intellectual property for organizations. How do you put value on a product that hasn't hit the market yet because it is still in the research and development phase?

What we try to help companies understand, especially from an investigative standpoint, is what information they have on their systems. The best way is to go through some form of an IT risk assessment and a business impact analysis. For instance, if that information was to get into the hands of an unauthorized individual, or information was leaked to an external website or hacking group, what is the value and financial impact?

What is the definition of social engineering?

Obuchowski: Social engineering could be a phone call to a company pretending to be a vendor asking for information relating to banking records or personnel questions like who is the new accounts payable rep or who's the new CIO or CFO? We tend to see a lot of phishing or social engineering emails.

Social engineering emails have become very targeted. It's not just a phishing email but a spear fishing email, where information that's used on public websites or social media or email communication from a company is used in order to craft a very specific correspondence targeted to an executive of a company or an employee to get them to do something that they normally wouldn't do.

What costs the most for companies after a breach?

Obuchowski: The costs do vary. The most expensive portion of an incident could be forensics because it could take two or three months in order to determine that there wasn't an incident. The regulatory fines can be very high, and it's hard to put a number on that.

If you have 20 million people that you need to notify that their information's been compromised, what's 20 million times the cost of a stamp? You hope to get to that person on the first round, but you're not going to get to 20 million people on the first notification. So it's these little things, outside of the forensics, like regulatory fines, lawsuits, and lawyers' fees that are associated with it.

What are typical questions that a client asks when they call you?

Obuchowski: If they're calling us it's because they are trying to plan ahead. They want to know what we are seeing in the market, what are we seeing in their industry, and what can we do to help. Help can come in the form of IT risk assessment, PCI compliance, social engineering training, or incident response training.

Risk assessments should be done up front because, with proper planning, the response is going to be more efficient and it will also make sure that we have, in some instances, the evidence that we need to help to determine what information has been compromised as part of that incident.

Is there such thing as an ironclad cybersecurity policy?

Obuchowski: If a company can survive without having any digital information and no email, then I would say they'd be in the ballpark of having an ironclad security policy.

We often hear about hackers breaking into a system and then saying they were looking to expose a weakness in a company's IT with the intention of being hired by the company they've breached. What usually happens in terms of prosecuting someone who does this?

Obuchowski: It depends on the organization. Anybody who tries to gain access or does gain access to a company's network or information without authorization is susceptible to state and federal laws. A person could be arrested depending upon how the organization wants to handle that incident and depending upon the information that was obtained.

What companies can do is hire ethical hackers. Those are people employed by legitimate companies in order to attempt to break into an organization's network and then let them know what information they were able to obtain. That could be done over the network or in person. To be successful, an investigator has to think like a criminal. "How would I gain access to this company's network? How would I steal information if I wanted to?" If you put yourself in that mindset, and couple that with years of experience and having the knowledge and information about the latest technology, they definitely become a very valuable resource. ■

> "If a company can survive without having any digital information and no email, then I would say they'd be in the ballpark of having an ironclad security policy."
>
> –Andy Obuchowski, RSM US LLP