Inside Counsel
SEPTEMBER 15, 2016
BUSINESS INSIGHTS FOR THE LEGAL PROFESSIONAL

An ALM Website
www.insidecounsel.com

BY JUSTIN HECTUS

Cybersecurity Beyond Traditional Risk Management

While some time-tested risk management concepts and strategies may be exactly the right approach for dealing with cyber risk, relegating it to a subset of anything speaks to a lack of understanding of the problem and will ultimately increase risk significantly.

AT A RECENT CIO PANEL, AN audience member asked the three of us on stage: "What do you see as your number one priority in the coming 12 months?"

It was my turn to go first, and I responded "cybersecurity" without hesitation. The panelist that followed said that cybersecurity was a priority, but that it is a subset of risk management, which is much more comprehensive and includes as a subset cyber threats and cyber risk management. This was not the first time I have heard the chief information pro and/or technologist in a large company make that point, and I have to respectfully disagree.

While some time-tested risk management concepts and strategies may be exactly the right approach for dealing with cyber risk, relegating it to a subset of anything speaks to a lack of understanding of the problem and will ultimately increase risk significantly.

The rapid pace of increasing complexity and the increasingly crippling impacts of cyber-specific threats demand a different degree of prioritization, resources and tireless attention than any other type of risk corporations face today. In the same way that technology will change the way we do business more in the next five years than any other catalyst, cyber risks will challenge our ability to operate more than any other threat.

It is against that backdrop that governments and large enterprises

have continued to harden their defenses and small to mid-sized businesses (SMBs) have lagged behind due to lack of resources or lack of motivation to mitigate risk. The prohibitive cost of comprehensive prevention measures and the frightening cost of breach response may lead many smaller companies to oversimplify the problem or to put their head in the sand hoping that no hackers pick on them.

While that may have been a safe bet a few years ago, it's becoming increasingly likely that being small doesn't keep you off the target list. According to Symantec's 2016 Internet Security Report, 43% of cyber-attacks target businesses with 1 to 250 employees — two and a half times the share attributed to that segment four years ago — making SMBs a growing sweet spot for bad actors.

Canaries in the Coal Mine

While the spate of recent high profile breaches in the legal industry and beyond may be dominating the headlines, there is an undercurrent of smaller scale breaches and attacks happening all around us. We have had first-hand experience over the past few months with smaller law firms being targeted and compromised by bad actors. The two most recent scenarios are outlined below.

In mid-July, several of our attorneys received an e-mail from co-counsel at another, smaller firm. The message had an Excel attachment. Recognizing that the content of the message and the attachment name seemed slightly out of the ordinary, one of the recipients sent a separate e-mail to the sender's known e-mail address and asked if the transmission was legitimate and stating that we are all being very cautious with unexpected attachments these days.

The response received was "*everything is fine over here and yes I sent the message, check it out.*" Our attorney was still skeptical despite the exchange and picked up the phone. Co-counsel said that he didn't know anything about the exchange and hadn't sent any e-mails to us in days. A hacker was logged into his actual account sending and responding to e-mails in a fairly convincing and targeted Man in the Middle (MitM) attack.

One week earlier, an attorney at our firm received a note from a partner at a 10-lawyer firm advising that they hadn't been able to review a pleading in a case we were trying against them because their entire system had been down for over two days. Ransomware had crippled their network and there was no clear ETA for return to full operations.

SMBs, including "Small Law," make great targets because they often lack sophisticated defense capabilities, but also because they don't believe they are high value target for attackers. What they may fail to realize is that the average ransom collected on infections is only a few hundred dollars and attackers are casting a wide net to get as many victims as possible, regardless of their size.

Also increasing the risk is the rise in MitM attacks which may leverage the little guy to compromise their larger partners or clients.

Failures on an Epic Scale

SMBs may be at particular risk, but they aren't the only segment of the corporate landscape failing to get the basics right. According to the United States Computer Emergency Readiness Team (US-CERT), the top targeted high risk vulnerabilities can consistently be solved by maintaining up-to-date software and patching commonly known vulnerabilities.

The Department of Defense Cybersecurity Discipline Implementation Plan, made public in March, doubles down on this, stating "most successful cyberspace intrusions exploit preventble and generally well-known vulnerabilities." Cisco's July 2016 Annual Security Report touched on the broad scope of the problem, finding that a startling 92% of Cisco devices in a recent survey were running software with known vulnerabilities.

Competing priorities and a shortage of budget and resources may contribute to the current state of broad-based weak security posture, but it's about to get much worse. As the economic benefits of hacking and attacking seem to be growing, the legislation and policy to prevent and respond to these attacks

seems to be stuck in the mud. *See*, "Ransomware Is the Most Profitable Hacker Scam Ever," *U.S. News*. Privacy concerns and a do-nothing Congress are at odds with a fast-changing threat landscape.

The head of U.S. Cyber Command recently all but begged members of the Senate Armed Services Committee "to accelerate debate on how to balance security and privacy in the ever-changing digital realm."

This is all against the backdrop of a severe shortage of qualified human resources to deal with the problems. While the U.S. government has outlined a strategy for training, hiring, and retaining cybersecurity talent and is in the midst of adding a total of 6,500 new cybersecurity pros, the demand for qualified professionals is far outpacing the supply.

In early 2015, estimates based on U.S. Bureau of Labor statistics indicated that there were just over 200,000 unfilled cybersecurity jobs in the U.S. *See*, "Demand to Fill Cybersecurity Jobs Booming," *Peninsula Press*. Intel Security's recent "Hacking the Skills Shortage" report projects that number to be one to two million by 2019. During the same CIO panel mentioned above, the head of a large global firm remarked: "If I wanted to hire another top-notch ITSec professional, I couldn't even do it right now."

Raising the Stakes

All of this paints a pretty bleak picture. The attacks are increasing in frequency, sophistication, and impact, we have a shortage of qualified human resources and legislation to help deal with the problem, and we consistently seem to be overlooking some easily fixable flaws that would prevent most attacks from being successful. But, hey, at least the only thing at risk is our data, right?

That turns out to be wrong (and possibly) dead wrong. The stakes are getting much higher and doing so much more quickly than you might think. As cyber physical systems come online and replace previously dumb devices with smart devices performing critical functionality in life safety, navigation and military applications, the high end of the risk spectrum changes dramatically.

Hackers have proven their capability to cause damage beyond simply compromising information security by remotely hijacking cars, triggering false alarms and opening the front door of smart homes, and even tilting a floating oil platform. Stuxnet's breakdown of the Iran nuclear centrifuges in 2010 may have been the first recorded major instance of a computer attack shutting down control systems and doing real world damage, but it certainly won't be the last. Someday we may look back and laugh at the recent period of major PII breaches, referring to that time as "the good old days."

The thought of credit card numbers or Social Security numbers being compromised quickly becomes inconsequential when a hack might result in significant injury or loss of life. That reality is upon us in limited instances now, and it will be our collective reality within the next five years.

Doomsday Preppers

If we're going to start getting this right, we better do it now. While not meant to be an exhaustive list by any means, here are a few good places to start based on the evidence of where we seem to be falling short.

Treat Cybersecurity as a 'Bet the Company' Issue

Don't treat cybersecurity as a subset of anything. This is an area of risk unlike anything businesses, especially SMBs, have ever faced. Ongoing identification and remediation of vulnerabilities and threats must be a priority unto its own. If you don't have the internal resources to do that, please see below.

Take Advantage of Outsourcing and Technology as a Service

Software as a Service (SaaS) has been a boon to SMBs. It used to be that you either had to act like a home user or you had to invest in enterprise systems. Today, SaaS solutions such as NetDocuments provide AmLaw 100 quality software (and security) at a price point that scales to the small firm and even solo practitioner.

Likewise, price flexes with size on services such as vulnerability assessment and penetration testing from companies such as Digital Defense

or EiQ Networks provide visibility to every end point and help even a layman patch or remove any vulnerability. And, if you want to know when someone is trying to get in or has gotten in, try a more holistic Security Information and Event Management (SIEM) approach from EiQ or Dell Secureworks.

These are all companies that provide "Security as a Service" that is a combination of field-tested professionals and world-class software.

Use Technology as a Force Multiplier

The bad guys have been doing this for over a decade. The difference is that they have improved their tactics, shifting from widely cast spam messages promising a cut of a princely inheritance to sophisticated algorithms that target their marks and triage response opportunities. They use analytics to set the price that victims will pay depending on the type of business they run.

Why should we expect that the old model of Antivirus+Firewall will keep us safe? Artificial intelligence and crowdsourcing are making a dramatic impact in recognizing and shutting down malware and viruses in real time, before traditional antivirus issues a pattern to detect and prevent execution of a dangerous payload. Solutions by Cylance and Carbon Black are taking unique approaches here worthy of their adversaries. It's no wonder that the VC community is on pace to invest $1.5B in companies in this space in 2016 alone.

Secure the Human Element

It's critical that your employees or coworkers understand the severity of the risk and their role in preventing compromise. Every employee with access to a computer has the responsibility to undergo training covering the risks associated with that access, and every employer has the responsibility to make sure that communication is timely and relevant and mandatory. Employees need to raise their guard and pick up the phone any time something seems out of the ordinary. If you want a good turnkey solution for that in place, check out Capensys' Sentinel, which can map to the LTC4 core competency framework. The cliché that you are only as strong as your weakest link has never been more accurate than it is here.

Get a Good Broker

The area of cyber insurance is evolving as rapidly as the threats it insures against, and insurance companies hold most of the cards. In addition to making sure you are well-covered beyond just the people, process and technology, working with an experienced insurance broker who specializes in cyber insurance coverage will give you an education about coverage available and the limitations or contingencies.

Even the process of going through the application can provide a litmus test for your cybersecurity posture, and the coverage can provide a safety net if an attack is so sophisticated that even the best defense is not enough.

There have been some interesting developments in this area in recent months and we will cover those in an article in a future column.

A version of this article originally appeared in Cybersecurity Law & Strategy, an affiliate of InsideCounsel.com.

CONTRIBUTING AUTHOR

JUSTIN HECTUS is the Director of Information at Keesal, Young & Logan where he oversees a variety of operational functions including the direction of the firm's IT vision, strategy and execution. A member of this newsletter's Board of Editors and a two-time ILTA Distinguished Peer Award winner, Justin and KYL have established a decades-long track record of effectively leveraging leading edge technology to achieve outstanding results on behalf of the firm's clients.