IT SECURITY

The Board Directors' Handbook

IT SECURITY

The Board Directors' Handbook

TABLE OF CONTENTS

Patrick J. Clawson
Information Security Leader, Author & Speaker

INFOSECURITY IS AN ENTERPRISE RISK

After a multitude of official warnings and too many high-profile data breaches that have impacted millions of customers, board members are scrambling to address IT security at their organizations. In fact, according to a recent study by FTI Consulting, Law in the Boardroom in 2014, data security is now the top concern among corporate directors and general counsel.

Has it hit your radar yet? What are you doing to manage the risk?

Today's hard truth is cybersecurity is a financial risk that impacts every business' bottom line. Regardless of your industry, company size or geography, attackers are either coming at you as a target or through you to target your partners. These aren't technology issues; they are core business issues.

For that reason alone, security should be managed the same as any other core business issue—with leadership from the top. The trick is not just prioritizing what was once left to your technical team but really understanding the risk and methodically working to improve the situation by aligning your enterprise infosecurity with overall business goals. Don't make security spending decisions from the bottom up, based on tactical concerns; make them as top-line business priorities.

Understand the issues. Set the tone for how security risks are managed.

THE HIGH COST OF CYBERCRIME

ACCORDING TO A 2014 REPORT BY THE CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

$445 BILLION

CYBERCRIME AND ECONOMIC ESPIONAGE COSTS THE WORLD ECONOMY AN ESTIMATED $445 BILLION — NEARLY 1 PERCENT OF GLOBAL INCOME

$100 BILLION

STOLEN INTELLECTUAL PROPERTY HAS COST THE U.S. AN ESTIMATED $100 BILLION

200,000 JOBS

MALICIOUS CYBERCRIMES ARE ESTIMATED TO COST AS MANY AS 200,000 JOBS IN THE U.S. ALONE

WHAT YOU NEED TO KNOW

Rather than let a lack of understanding stop you from managing this critical risk, dive into the issues. In the following sections, I'll explain the three truths you need to understand about IT security to get started. They don't require translation from your technical team and they are immediately actionable.

As a board member, you have the visibility and authority no one else has. You see the company holistically. You know which at-risk assets mean the most to the company. And you know that it's your name and reputation on the line when a breach hits the news. Don't just hope others will come up with a security plan that covers the most important risks to the bottom line. Be the catalyst to drive real change.

WHAT BOARDS ARE SAYING ABOUT THEIR CYBERSECURITY REPORTS

IT GOVERNANCE LTD., *BOARDROOM CYBER WATCH SURVEY 2014*

33%
say their boards receive no regular reports on cybersecurity

21%
believe their board reports fail to provide the information necessary for boards to make decisions

29%
believe that fear of retribution might be discouraging IT to fully disclose details

RISKS HAVE EVOLVED

The ABCs of APTs

Security threats aren't really about technology at all. Your biggest threats aren't malicious code, botnets, infection rates or even spear phishing. These techy terms are all symptoms of the greater risk to your enterprise: theft and business disruption.

Stealing from your business has become the bad guys' business – they are making buckets of money attacking you. They've also upped their game immensely during the past few years. These days they're targeting specific industries, specific companies and even specific employees to achieve precise black market business aims. Security pros have a short-hand term to describe the targeted attackers that have upped the ante on our cyber risks: APTs. Advanced Persistent Threats.

Their goals could be to steal your most valuable intellectual property, plunder your bank accounts, traffic large stores of your customer data, act as mercenaries gathering intelligence about your firm for nation-states or generally discredit you as a viable business entity.

The payoff is high for these targeted attackers, so they're persistent. They're researching your company's weaknesses and they're investing in automated technology to exploit them.

HOW & WHY

40% 40% of respondents say their endpoints have been the entry point for an APT/ targeted attack in the past 12 months

95% Financial motives now drive nearly 95% of cyber-attacks

Whether you have mechanical blueprints or software code, customer data or confidential partner information, if it's valuable to you, it's valuable to hacking thieves. And they'll stop at nothing to steal that valuable data. They might throw distributed denial-of-service (DDoS) attacks at your network to distract you from an infiltration somewhere else. They could automate technical exploits of vulnerabilities in your website software to gain access to sensitive databases.

Mostly, though, they're going to go after one of your least obvious technical vulnerabilities: employee laptops, tablets and smartphones. Security isn't just a matter of flipping a technological switch. It's about managing risk—and the biggest cyber-risk today is rooted in employee ignorance and computing negligence.

PORTRAIT OF AN ATTACK

1. Sophisticated, malicious organizations develop a strategic attack plan for you, methodically looking for your vulnerabilities.

2. Once they have identified a possible path, they build a malware payload and distribute that payload with instructions to exploit.

3. Once you're exploited, the payload will phone home and allow the bad actors to establish command and control over your network.

4. The malware continues to expand its footprint in your system and possibly execute across multiple vulnerabilities.

HOW DO TARGETED ATTACKS START?

2014 STATE OF THE ENDPOINT STUDY, PONEMON INSTITUTE

45%	34%	33%	21%	12%	33%	33%
spear phishing emails sent to employees	web-based click jacking	fraudulently signed code/ digital certificates	memory-based attack	SQL injection code	USB key delivery	unsure/other

COMPLIANCE DOES NOT EQUAL SECURITY

Just because you're making it over the compliance bar doesn't mean you're actually clearing security hurdles. Compliance with standards like HIPAA, SOX and PCI DSS shows how you stack up against established standards. It's not necessarily a measurement of overall risk management. As you probably have read about, many of the organizations that have suffered high-profile breaches were in compliance with various standards.

Look at the recent breach at Target. The company claimed it was PCI-compliant when the incident occurred. Even if that's true, compliance didn't shield Target in the court of public opinion. The retailer has seen fluctuating stock price all year – with an opening price of $63.55 the day news of the breach broke and dropping all the way to $55.12 in February. By the end of Q3 2014, TGT has yet to hit its pre-breach price. Customer-satisfaction levels fell following the breach and more dramatically, the fallout from the breach saw dire executive level consequences, with the ouster of the company CIO and later, the CEO. To be sure, PCI compliance won't shield your organization if a similar breach happens to you.

I tell my fellow executives all the time: Draft a security program that meshes security practices against the risk profile of your specific organization, without dwelling on pleasing the auditors.

You can't fight today's threats with yesterday's strategies. What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries.

Gary Loveland
Principal
PwC's US Security Leader

Target's customer satisfaction ratings among upper-income shoppers dropped 9 percentage points following its breach.

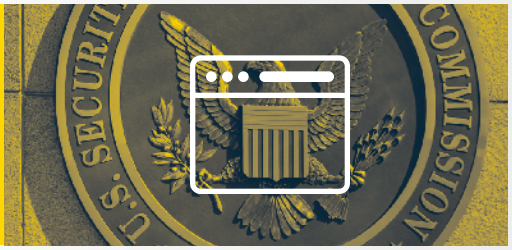
Cowen & Co. Consumer Tracking Survey

COMPLIANCE DOES NOT EQUAL SECURITY (CONTINUED)

SEC Guidance for Publicly-traded Companies

Publicly traded companies should already be following SEC guidance issued in 2011 for financial disclosure if a breach leads to reduced revenue or higher costs that could cause stock price fluctuation. In 2014, the SEC has been tightening the reins and, in April, announced their plans to examine cybersecurity preparedness at more than 50 broker-dealers and investment advisers. In the midst of that announcement, they released a checklist of requests they may ask these broker-dealers.

Regardless of what comes out of the SEC in the future, this checklist is worth a look. You can read the thought-provoking document here.



COMPLIANCE FINES VS. SECURITY INCIDENT COSTS

2014 COST OF DATA BREACH STUDY, PONEMON INSTITUTE

Addressing risk before compliance isn't just a safer and saner way of doing things—it is also the most cost-effective approach.

Compliance fines pale in comparison to the cost of an actual security incident that can occur when proper precautions are not put into place. If an otherwise compliant organization misses a certain piece of the security puzzle and suffers a huge breach, then it stands to lose a lot more in lost revenue than had it been secure but noncompliant.

$5,850,000 Average cost of breaches to organizations in the U.S.

$417,700 Detection and escalation cost per breach

$509,237 Notification costs

$1,599,996 Legal expenses, client communication, after-the-fact costs

$3,030,000 Lost businesss

WHAT YOU NEED TO DO

Thankfully, addressing information security is more than throwing cash at the problem.

Many IT professionals get so hung up on the technology that they forget their security priorities should be based on business risks instead of technology threats, particularly when no one above them is offering them business context for their operational decisions. The most important piece of advice I can give is four-fold. First, use your best effort to understand what these malicious organizations are after. Second, make them work harder by reducing your known attack surface area. You know they are coming for you so clean up your low-hanging fruit like updating to the newest operating system, for example. Third, ask yourself, how many layers of protection can I put between my data and the bad guys? There is no one technology silver bullet to keep everyone out. Finally, add follow-up to your overall strategy. You will be breached at some point; no one is immune. When that happens, dissect the situation, learn from it and prevent it from happening again.

IT security is not just a technology problem.

IT security is best addressed through people – your employees, your partners and your vendors – the implementation of strong process and smart technology. Tell your CEO you are committed to this approach.

Train People for Success

Human nature says that employees and trusted partners with access to your information will take risks if they aren't aware they're doing so. Ongoing education is hugely important because as we all know telling employees not to do something doesn't always fix the problem.

It is the job of your information security department to make people understand why they can't do whatever they want with their work computers. And it is your job as a board member to back up the CEO and CISO and when they are outlining process.

One hundred percent security will never be possible, so what you have to do is really focus your spend in the areas that are most important to the organization.

Steve Durbin
Executive Vice President
Information Security Forum

WHAT YOU NEED TO DO
(CONTINUED)

Set Process Through Risk-based Policies

Tuning security processes to business risks is the hardest part of IT security. It's also the most important part and the one in which key board members should play the biggest role.

The keystone is a solid risk assessment. An effective risk assessment combines your inside knowledge of business initiatives with your tech leaders' knowledge of the most pressing technical threats. This synergy allows everyone to rank risks based on their impact to the business and make security spending decisions that are based on business needs.

Invest in Technology

Obviously, education and process development is only a start. You also have to require automated checks and balances to make sure these measures take within your organization. Technology that automates policy enforcement, smart monitoring technology and effective user controls should serve as a backstop for your people and process prep work.

And while we are talking technology, it's important to remember there is no one silver bullet. You need multiple layers of defense, just as the bad guys try multiple points of entry. The idea is to never rely on a single security technology to keep you safe. You need to layer different types to fill all of the gaps left behind by each individual security stratum and make it harder for the bad guys to breach. If it's hard enough, they might just pass you by.

THE MOST EFFECTIVE POLICIES & PROCESSES

According to the SANS Institute

Identify the assets that are most important to critical business functions

Identify all of the vulnerabilities to those assets and the likeliness of the threats to exploit them

Prioritize activities based on the most important business assets, most critical vulnerabilities and highest likelihood of threat impact

Build in monitoring and review procedures to improve processes along the way

HOW TO LEAD SECURITY FROM THE TOP

Ernst & Young's *2013 Global Information Security Survey*

Articulate risk appetite to provide clear, unambiguous direction

Understand how security events can impact the business, its services and its products

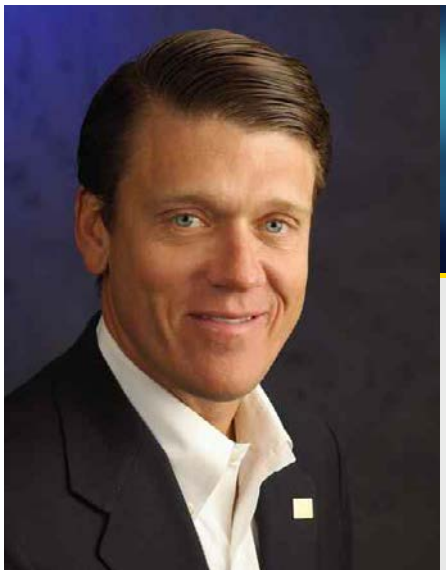
Incent timely remediation of security issues

Integrate information security insights directly into management decision-making processes

Measure information security performance and the criteria for success

Translate information security threats into their impact on the P&L and balance sheet

Foster an information security culture throughout all levels of the organization



IT SECURITY
The Board Directors' Handbook

Patrick J. Clawson

Patrick J. Clawson is an information security leader, author and speaker. He served as Chairman and CEO of Lumension Security, Inc. where he drove the company's strategic direction and revenue growth prior to its sale to Clearlake Capital, LP.

With 25 years of software industry experience and running high tech companies, Clawson has extensive experience in both domestic and international sales, marketing and operations. He is a frequent speaker, publication contributor, infosec blogger and four-time entrepreneurship honoree by Ernst and Young.

Prior to joining Lumension, Clawson served as Chairman and CEO of CyberGuard Corporation, a security software company, where he spearheaded the launch of new technologies into the marketplace and oversaw the integration of more than four key acquisitions. He served on the board of directors for e-DMZ Security during its significant growth and subsequent sale to Quest Software and then Dell and Prolexic, sold to Akamai Technologies. He also serves on the Board of Directors for K is for Kids, a unique student-volunteer based charitable organization based in Naples, FL.