CISOs struggling to take the risk out of risk

There is risk everywhere, but how can a CISO reduce the company's risk profile without accidentally introducing even *more*? Evan Schuman reports.

The very essence of an enterprise risk strategy is intermingled with both security and compliance. But if security and compliance were in a kindergarten class together, both would get a failing grade in "playing well with others." At least such a grade would be merited by the way so many Fortune 1000 companies not only fail to coordinate the two adequately, but they often pit them against each other with C-level edicts that seem to pretend the other group is irrelevant.

This lends to jurisdictional overlap, which has the mirror consequence of allowing some priorities on each side to fall through the corporate cracks because each mistakenly assumes the other side is handling it.

Kurt Lieber, the CISO for $2 billion healthcare insurance company Aetna, says that he finds compliance — which should reinforce security by providing basic rules for companies to meet — often undermines rather than reinforces cybersecurity.

"For the industry, it is somewhat frustrating to be so reliant on compliance," Lieber says. More often than not, "compliance becomes more of a distractor than an enabler."

Not only are regulators not especially sympathetic to security's struggles in Lieber's view, but those regulators are often not especially accommodating when some of a company's regulation conflicts with other regulations. When a company explains why it chose to adhere to a conflicting regulation, regulators "don't react very positively," Lieber says.

Lieber says the biggest risk threat he sees today comes from government agents of countries outside of the U.S. "The biggest risk hurdles will be the emergence of nation states in the playing field of the threat actors," Lieber says. "We saw it with Stuxnet. It sort of upped the game for everybody."

For Aetna, Lieber says, the nation state threat convinced management that it needed to embrace artificial intelligence machine learning as a way to make automatic response quickly — without human intervention — to attacks. "For us, it pointed to a need to be moving at machine speed," Lieber says, acknowledging that some companies have been hesitant to allow software to make response decisions autonomously. "I don't know that we have the choice. It's not a question of 'Should we?' It's 'How do we?'"

Much closer to home for Aetna, however, are a range of healthcare-related security risk issues. He cites the business-to-business (B2B) digital payments issue as an especially crucial one for healthcare concerns, considering the many non-hospital staff physicians who bill themselves as third parties, often as part of a medical group. "Healthcare is one of the poster children" for B2B digital payments, Lieber says.

Another healthcare vertical concern is the

OUR EXPERTS: RISK STRATEGY

Richard Diver, cloud security architect, Insight
Chris Duvall, senior director, The Chertoff Group
Chris Krueger, principal, Coalfire
Kurt Lieber, CISO, Aetna
Christopher McClean, VP and research director, Forrester
Emily Mossburg, risk and financial advisory principal, Deloitte & Touche
Sam Olyaei, senior principal, Gartner

Risk strategy

56%

Percentage of IT pros who said targeted phishing attacks were their top security threat

– CyberArk Global Advanced Threat Landscape Report 2018

move to electronic health records (EHR), also known as electronic medical records (EMR). "From a security standpoint, the [move to EHR] was a disaster," Lieber says.

He also cites Flexible Spending Accounts (FSA) — a government mechanism for setting aside payroll money to cover employee health costs pre-tax — as another security problem. Cyberthieves could steal money from those accounts with a lot less chance of being detected, he says.

"For all intents and purposes, these are bank accounts but they are managed by health companies. And they don't have a lot of experience taking care of these things," Lieber says. "How often do you check your

The stuff that has always been harmless should scare you

Here is a frightening thought for CISOs examining their risk strategies: The biggest security threats have historically come from systems that have been around for decades and have always been utterly innocuous. But when they get upgraded just a little, they can quickly become a massive data leak.

The most notorious historic example was when peripherals — mostly printers, along with some fax machines and scanners — became smart and got their own IP address so they could be accessed throughout the enterprise. They quickly became a cyberthief's best friend, as it provided an entirely open backdoor access to the network. Once discovered, that hole was quickly plugged, but not until many companies spent months and sometimes years exposed.

More recently, the internet of things (IoT) gave antennas and network access to historically safe devices such as lightbulbs, IP security cameras, coffee pots, and aquarium heaters, allowing them to share data outside the network with their manufacturers — and anyone who could trick the IoT devices into believing they were the device's manufacturer. Considering the lack of built-in cybersecurity, combined with the dearth of products that support security updates, these perhaps not-so-smart devices pose a significant risk and introduce considerable network vulnerabilities.

The latest sneaky threat comes from business-to-business (B2B) digital payments. Moving from checks to electronic funds transfer transactions is safe enough, but today's more sophisticated B2B digital payment deployments include far more information. It is not just the name of the payee (typically suppliers, distributors, contractors and employees), but it can now include the date the purchase order was issued, the name of the person who authorized it, the name of the supervisor who approved it, comprehensive details of everything being purchased, a copy of the contract, a copy of the invoice, and more. In a healthcare environment, it might include the name of the patient for whom this work was performed, the nature of that patient's condition and other details that would make a HIPAA regulator have a cardiac arrest.

Furthermore, those B2B digital payment details are not solely shared with the payer and the payee. That data is routed to the bank of the payer and the payee, a payment processor, potentially a payment facilitator and even possibly other payees. The amount of data being shared, and the number of people who might gain access to it, soar with digital payments.

So when your company moves to B2B digital payments, is your risk plan updated? How long did it take before risk acknowledged IoT? Smart printers? The more things change, the more the risk *does not* stay the same.

—ES

70%

Percentage of companies that said their risk increased in 2017

– Ponemon

FSA account?" he asks rhetorically. "Much less often than you check your [traditional] bank account."

Repeating mistakes

Other security experts identify additional factors in the vastly increased threat and risk landscape today.

Chris Duvall, senior director, The Chertoff Group

Chris Duvall is a senior director at The Chertoff Group, a Washington, D.C.-based security consulting firm co-founded by former Department of Homeland Security Sfecretary Michael Chertoff. Duvall argues that one of the risk roadblocks is how understaffed many enterprise security and IT teams are currently. Often, understaffing and overworking can lead to some very bad security habits, Duvall says.

"IT folks can be overworked, ill-prepared or lazy and just decide to concentrate on other activities rather than slog through patching X thousands of Windows, Linux, iOS operating systems and apps. If you have 10,000 critical vulnerabilities across multiple regions, where do you start?" Duvall asks. "How do you avoid the dreaded 'down time' the business units scream about while trying to patch and test? How do you finish before the next 'Patch Tuesday' before it all starts over? Some just say 'Screw it. We'll wait until we replace/upgrade it and make sure that version is secure.'"

> "CISOs need to talk at a more strategic level, and to speak more in a non-technical way for other departments"
>
> *– Chris Duvall, senior director, The Chertoff Group*

Sometimes, Duvall says, the lack of preparation or drive can be a result of a deficiency of proper training. Duvall says he has seen "IT staff that don't know what they are doing and so they just don't do it. Patching is a common example. It's hard, especially for legacy machines and so sometimes folks just ignore it."

Another concern he expresses is the rapid expansion of use of APIs. "Nobody is really keeping track of those and they are potentially easy channels right into the network or an individual toolset," Duvall says.

If a company does not practice good backup hygiene, it can allow itself to be attacked repeatedly by the same piece of ransomware. The first time is when the malware originally launches and then again when the company reinstalls data and programs from a file or image backup and inadvertently re-infects their own systems. The appropriate approach is to ensure the backup itself is malware-free before restoring the image or file. Often malware that is dormant can end up being included in a backup process; if the backup itself is not scanned and decontaminated before a restore, the malware can simply launch itself again and again.

Duvall also expresses concern that even today, with multiple news reports about corporate laptops being stolen from cars and airports, "folks are still debating whether they should have full-disk encryption."

Another worry is intracompany communications with security. "CISOs need to talk at a more strategic level, and to speak more in a non-technical way for other departments," he says, adding that CISOs should steal a play from the development, security and operations (DevSecOps) teams and embed security staffers into

#1

The top cybersecurity risk to US businesses is employee negligence

– Shred-it

other departments, then rotate them back to security so that they can act as a representative of other departments.

But perhaps an even greater risk, Duvall says, is the lack of identity centralization for many enterprises. "So often, they've got 15 [or] 20 separate domain IDs that they haven't audited. You need to lock them down ASAP," he says.

Emily Mossburg, risk and financial advisory principal, Deloitte & Touche

Why? Privilege auditing, making sure that access to specific servers is kept current, is often a priority for terminations and for people who voluntarily leave the company, but much less for someone who is transferred and especially if those people are promoted. "As folk are transferred, you really need to hunt that down," he says.

A key concern that many cite was the neglect of security issues when transferring systems to the cloud.

Insomnia

"What keeps me up at night is the possibility of the missed opportunity to do this right from the beginning," says Emily Mossburg, risk and financial advisory principal at Deloitte & Touche. "As an [enterprise] shifts from an on-premise model to one that leverages the cloud, the risks — and therefore the overall set of cyber risk requirements that they need to consider — shifts and changes," she says.

Mossberg notes that companies need to ask the right questions. "Are [enterprises] recognizing how dramatically their risk profile is shifting — not necessarily increasing but changing? And are they designing the new environment with those changing requirements in mind? Or, are they replicating the mistakes they've made in the past as they build the legacy infrastructure and moving those to the cloud?" These, she notes, are among the questions companies need to consider.

Chris Krueger, the principal for cyber engineering at cybersecurity consulting firm Coalfire, argues that his big issue with many of today's cloud deployments is that security is an afterthought. "I observe a similar 'add security later' mentality in many hyper-scale cloud projects that plagued on-prem and hosted [efforts] during the previous two decades," Krueger says.

"I'm also seeing management and the [board of directors] not properly include cybersecurity assets in their project budgets and planning," he continues, "and cloud-DevOps teams who are just building credibility in conventional IT organizations [while] not painting the big picture of costs, risks, and rewards. Lessons of the past [are] being re-learned in fresh blood and at hyper-scale."

In short, Krueger's key cloud fear is that too many large companies are "relying way too much on their legacy environment as a frame of reference. Between the development care and the upkeep, [the cloud] necessitates a whole new team." At the same, Krueger argues, [they] are insufficiently leveraging what a cloud is offering as platform-as-a-service.

> "What keeps me up at night is the possibility of the missed opportunity to do this right from the beginning"
>
> *– Emily Mossburg, risk and financial advisory principal, Deloitte & Touche*

A big part of this is long-term versus short-

77%

Percentage of attacks that compromised companies in 2017 that used fileless techniques

– Ponemon

term thinking, which is especially problematic considering how often CISOs typically change jobs. A 2017 report from Enterprise Strategy Group and the Information Systems Security Association (ISSA) titled *The Life and Times of Cybersecurity Professionals* says CISOs typically change jobs every two to four years. If the CISO is not anticipating being at that company more than a year, it might be more difficult for them to invest their budget in something that will not deliver rewards for three years — well after they have left the company. Other than offering CISOs incentives that live well beyond their employment, think of the stock options model but without the stock, there is not that much an enterprise can do about that problem.

Chris Krueger, principal, Coalfire

As an example, Krueger points to log analytics. "There are great advantages to the way some clouds do log analytics" and they translate into long-term advantages to the company if they will use those analytics natively from the cloud, he says. But that might require new training and other investments to make the switch. Would a CISO planning to take a new job consider launching such a program?

> "From a security standpoint, the biggest risk companies will run into is assuming that on-premise procedures will carry over. In most instances, they simply can't."
>
> – Kurt Lieber, CISO, Aetna

"To jump ship and all of a sudden use [a new logging analytics suite is] non-trivial but it may be worth it in the long term," Krueger says. "You may have 20 people who are trained in your legacy [analytics]. Due to the knowledge base, they think it may not be worth the change," he says.

An aggressive approach to risk

Aetna's Lieber agreed with Krueger on the cloud risks. "From a security standpoint, the biggest risk companies will run into is assuming that on-premise procedures will carry over. In most instances, they simply can't," Lieber says.

"Patching is a great example. With cloud rehydration, you don't patch anything, you just rebuild it. Your patching problem has gone away. In some respects, the cloud gets a bad name," he notes.

Richard Diver, the cloud security architect at security consulting firm Insight, concurs. "We're seeing companies continuing the same bad practices that they have always done on-prem."

Another major risk concern identified by Deloitte's Mossburg's involves how businesses are structured to handle both security and compliance. Often, she sees security using one customized framework while legal and regulatory and standards use different frameworks "and then the internal audit organization is not on the same page. Sometimes, the proactive conversations and the sharing that would minimize this kind of conflict doesn't happen. The language and the nomenclature [from various departments] are different."

This confusion and overlap results in "wasted time, wasted effort and confusion within the business units," Mossburg says. It can specifically cause senior executives who are reviewing all of these reports to get confused about whether or not the company is truly compliant.

Also, she continues, CISOs "are leaving

39

There is a hacker attack every 39 seconds affecting one in three Americans

– Cybinit

themselves open in certain areas. If you are spending this much time in [one area], that time and effort isn't being spent where the gaps are."

Christopher McClean, a Forrester VP and research director, encourages CISOs to take an aggressive approach to risk. "I heard

> "CISOs today are being held accountable for risk that they don't own"
>
> – Sam Olyaei, senior principal, Gartner

about a CISO client this morning whose new goal is to help his consumer electronics company take on more risk. Now that's a change to risk strategy that will determine what they do about IoT, not the other way around," McClean says.

But McClean echoed the concerns about company structure in the battle over security, compliance and audit. "Audit typically asks the same questions that the other two groups just asked," McClean says.

Insight's Diver sees a key issue involving cloud migration: IT executives purchase cloud platforms without fully investigating and understanding the capabilities of what they just purchased. "We spend a lot of time helping customers understand what they already bought" and that invariably leads to a security problem related to "the failure to implement something they've paid for."

Sam Olyaei, a Gartner senior principal focusing on security and risk management, sees the CISO risk problem as even broader. "How can CISOs balance the need to run the business against the need to protect the business?" Olyaei asks. "CISOs today are being held accountable for risk that they don't own," such as human resources risks. ■

For more information about eBooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an eBook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

$38.5B

The most expensive computer virus of all time was MyDoom

– AV-Test GmbH