Accenture Security

MEASURING THE COST OF CYBER CRIME: IMPLICATIONS FOR FY18 CYBER DEFENSE INVESTMENTS

ACCENTURE CYBERSECURITY FORUM VIRTUAL ROUNDTABLE SUMMARY

December 12, 2017

Measuring the cost of cyber crime: Implications for FY18 cyber defense investments

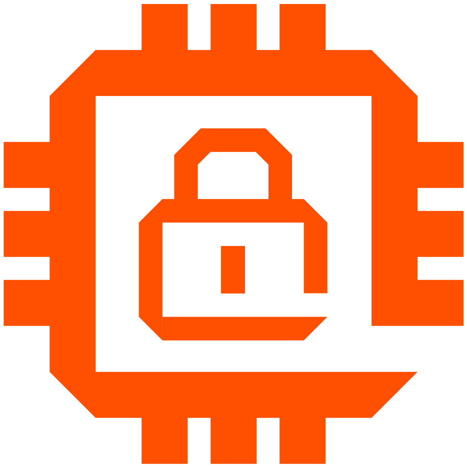
WHERE TO PRIORITIZE CYBERSECURITY SPENDING FOR THE MOST IMPACT

The most recent Accenture Cybersecurity Forum roundtable looked at results of new cyber crime research and the implications for cyber defense investments.

The discussion focused on the effectiveness of various cybersecurity technologies in limiting the costs and impacts of cyberattacks, and where to prioritize spending to make the most difference. As Accenture CISO and forum host Andy Vautier observed, such guidance offers real value in a world where threats and capabilities constantly evolve, but budgets remain constrained.

Cybersecurity executives from multiple industries attended the roundtable, conducted under the Chatham House Rule: All forum members are free to use the information shared, if neither the identity of the speaker nor the speaker’s organization is revealed.

NEW CYBER CRIME RESEARCH: RISING COSTS AND MORE BREACHES



Kevin Richards, Accenture Security North America lead and subject matter expert for the roundtable, opened the discussion by sharing highlights of the “2017 Cyber Crime Study,” independently conducted by Ponemon Institute LLC and jointly developed by Accenture.

The study, conducted with 2,182 respondents in 254 organizations in seven countries (Australia, France, Germany, Italy, Japan, United Kingdom, and United States), showed that organizations experience an average of 130 successful infiltrations per year, at a global average annualized cost of almost US$12 million.

The cost per organization has increased 47 percent in the past four years, Richards said, while the number of breaches has increased 91 percent in the past five years.

Costs, he explained, are those to detect, recover, investigate, manage, and remediate the exposure from an infiltration. “These are the costs of identifying when the malicious event happens, and the cost to get it out of the infrastructure,” he summarized. They do not include valuation of assets lost (addressed in a complementary Ponemon study on “Cost of a Data Breach”).

Phishing and malicious code attacks continue to be among the leading types of cybercrime, according to the study, and ransomware is seeing “significant orders of magnitude growth,” Richards noted. The research also showed that it can still take months to identify malicious activities.

ASSESSING CYBERSECURITY SPENDING

The research looked at where organizations invest in cyber defense, and the return on that investment. As Richards put it, “Where are we spending money? And are we spending money on the areas that actually will allow us to reduce cyber crime?”

The study found a significant gap between the spending priority placed on areas such as perimeter controls, and governance, risk management and compliance (GRC) technologies, and the relative cyber-crime cost savings they deliver. Investment in breakthrough technologies with even greater security potential—such as AI orchestration and machine learning or advanced behavioral analytics—has been significantly less.

He summarized: “We found something that was really interesting, because we saw that a lot of the spend has been focused on those areas that have traditionally been audit-driven. But when we overlaid the technology that could actually stop cyber crime, that was where the lowest amount of spend was happening.”

Organizations have an opportunity to rebalance and reprioritize their cyber defense investments so that important audit requirements are met while overall risk posture is improved. “We're seeing opportunities for organizations to spend wiser and reallocate funds from those things that are consuming energy and time and are maybe not being as effective as hoped, and reapplying them to those areas that can actually reduce the cyber crime exposure,” he said.

One potential source of freeing up funds is tool proliferation. “We're seeing in the security space the kind of tool sprawl that IT organizations have been struggling with for some time,” Richards said. “That creates opportunities for enterprises to undertake rationalization programs.” Organizations can create an inventory of their portfolio of tools and then consolidate—to cite a simple yet common example, go from multiple antivirus programs in the enterprise to just one or two.

INVESTING IN SECURITY HYGIENE VERSUS SECURITY INNOVATION

In the quest to prioritize investments, balancing security hygiene and security innovation is an important consideration. Organizations can feel tempted to “chase shiny objects” in the cybersecurity toolkit, Richards noted, but this should not come at the expense of encouraging and rewarding investment in fundamental security protections. The challenge is how to be technologically advanced yet also “understand how the attackers are coming at us” and defend accordingly.

As the CISO for a pharmaceuticals company observed, “There's an interesting balance between making sure you do your hygiene well and not doing that because you're off chasing the shiny new toy, whether it's CASB (cloud access security broker) or something else. Sometimes the hygiene does not get done, because of the shiny toys.” Organizations need a two-pronged approach, balancing hygiene and innovation.

Ironically, funding can sometimes be easier to win for security innovations than security fundamentals. As a data services CISO pointed out, “The shiny new objects are what leadership tends to like and want to hear most about, and oftentimes they are budgeted for easily. They see it, hear about it, and say yes to it. But for something less glamorous, like a tool that can make our de-provisioning process 25 percent more efficient or effective, the reaction might be, ‘Why are you spending money on that?’—even though it has a far more impactful benefit to the overall organizational security posture.”

Richards brought up the example of creating an inventory of endpoint assets, an important but decidedly unglamorous security basic. In conversations with C-suite and board executives, he said, “they find it incomprehensible that we as CISOs struggle with getting an asset inventory. Organizations know how many manufacturing devices they have, or how many offices they have. Leadership can’t understand why we don’t know all of our endpoints. So sometimes the reason hygiene isn’t attractive is that leadership assumes you have already figured it out.”

The CISO for a global healthcare organization suggested “a back to basics approach” for justifying the cost of non-glamorous security investments: clearly laying out the business case for why they make sense. “Quantifying an approach makes it much easier to go to members of the board who may not be technologically astute but who have sharp business sense to help them understand how best to make our investments,” he said.

The CISO for an IT services enterprise recommended what he called a “hybrid approach” of bundling the fundamental and the innovative together in funding requests. “We have succeeded in securing the investment dollars we need for improving and maturing the fundamentals by bringing in some of the new and shiny,” he said. “Server patching, for example, is built into our cloud transformation efforts. Improving mobile protections is built into productivity improvement. There are ways to tell the story that combine market- relevant buzzwords with the need to get the fundamentals right.”

He added, “Candidly, that's what the bad actors are going after—the fundamentals, and any weaknesses that are exposed. Protecting those creates a higher level of security for the company.”

”

CANDIDLY, THAT'S WHAT THE BAD ACTORS ARE GOING AFTER—THE FUNDAMENTALS, AND ANY WEAKNESSES THAT ARE EXPOSED. PROTECTING THOSE CREATES A HIGHER LEVEL OF SECURITY FOR THE COMPANY.

Kevin Richards

SECURITY INVESTMENTS TO PRIORITIZE

Flaws in security hygiene are the most common entry points for cyber criminals. “The organized crime threat actors are not super innovative,” Richards explained. While there are “zero day” attacks, particularly from nation states, criminals persistently use known malware and exploit known vulnerabilities. They take advantage of organizational lapses in security hygiene.

Defending against those common threats, whether through a fundamental security practice or an innovative technology, must be a priority.

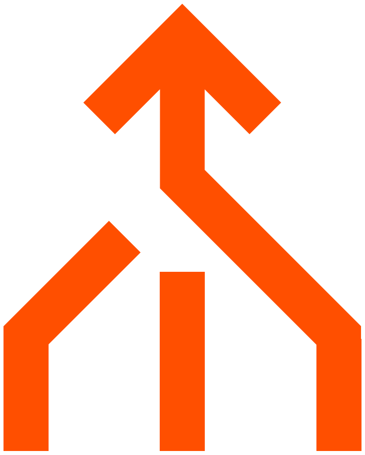
One investment worth prioritizing is new intelligence and automation technology that enables machine-to-machine decisioning in milliseconds or nanoseconds to block “known bads” automatically. “These are the commodity things that we know about,” Richards said. “If it's a known bad, block it. You don't need to go ask someone first.”

Another priority technology is advanced identity management. Driving identity decisions to the transaction level, even through simple techniques like texting a code to the phone of the requestor, “will stop an extremely large number of these attacks,” Richards said. “We have been talking about these things for years, and now we actually have the technology to do it.”

The CISO from a technology manufacturing company raised concerns about how to prioritize assets, as well as how to protect cloud-based assets, which led Richards to recommend another priority investment for preventing cyber crime: behavioral analytics.

“The thing I'm trying to figure out is prioritization,” the technology CISO said. “If you have an ocean of assets, how do you go after what is critical and protect them? The other thing is about how easy it is to steal information from cloud assets—especially the file shares that are cloud based, and how control for the file share is democratized and passed to end users who don't have the same discipline of worrying about security like the IT people do.”

Richards commented that, with respect to prioritizing assets, the issue from a security perspective is “understanding what matters the most, where it lives, and who should have access to it.” Regarding cloud-based assets, he agreed that special challenges come up, especially as corporate and personal sharing sites intermingle. Each of these areas requires careful governance around access management.



He pointed out that much of the risk involved with high-value and cloud-based assets has to do with the people accessing them. “From an attacker perspective, there is a significant amount of spear phishing that goes on. In many scenarios, they spear phish key individuals, high-value targets.” If successful, the attacker then “siphons off” information hoping that something of value will ultimately be obtained.

“Those incidents are very, very hard to detect,” Richards noted, “but we are seeing big improvement on endpoint technologies that aren't signature based. The new technologies aren’t looking to match saved file patterns, they're looking for anomalous behaviors in system memory and processes. They use behavioral analytics at the endpoint.” Such technology is worth considering, he suggested, because when it comes to cyber crime, “we see more leakage out of hacked individuals than we see from the cloud provider being hacked.” Structuring detection and remediation at the behavioral level recognizes that reality.

Intelligent systems, advanced identity and access management, behavioral analytics— all are technologies worth prioritized investment, in Richards’ view, not because they are transformational, but because they are practical. “It’s just readjusting,” Richards said. “It's not big, huge brush strokes. These are fine-tuning corrections. We have to recognize the need to change. And then we need to push these technologies. They are readily available, so now it's a matter of making it reality.”

BENEFITS OF **OPTIMIZING SECURITY SPENDING**

Reprioritizing investments, and achieving a balance between hygienic and innovative solutions, is more about optimizing than reducing cyber defense costs.

“Reallocating based on wiser spend, undertaking tools rationalization, focusing on key areas that have a bigger impact—that's going to free up funds that can be then applied to projects that you had put below the line,” Richards said. “While I wouldn’t want to suggest that these steps will create a windfall back to the business, they will allow us to get more done, raise the bar from a capability perspective, and lower the risk to the enterprise.”

The CISO from a financial services organization suggested one other consideration to aid in prioritizing investments—quantifying the value of assets and information. “Once you have quantified the high-value asset and high-value risk, you can now talk about value at risk,” he explained. “If there's a critical vulnerability on a high-value asset, we can now put a monetization on what is the value at risk. We can now share that with the business, and determine if they want to remedy it, or accept it.” The visibility makes investment decisions more informed.

> **REALLOCATING BASED ON WISER SPEND, UNDERTAKING TOOLS RATIONALIZATION, FOCUSING ON KEY AREAS THAT HAVE A BIGGER IMPACT—THAT'S GOING TO FREE UP FUNDS THAT CAN BE THEN APPLIED TO PROJECTS THAT YOU HAD PUT BELOW THE LINE.**
>
> **Kevin Richards**

THE EVOLUTION OF CYBER CRIME

The final topic in the discussion concerned the evolution of cyber crime and how organizations should respond. Richards recommended seizing one clear advantage that organizations have over cyber criminals: “We know what's important to our business, we know where the assets live, and we know what applications are there. The bad guys have to figure that out. We actually have a little bit of a head start, and we have to take advantage of it.”

But, he warned, “Don't underestimate the sophistication of the attackers. It could surprise you how structured, functional, and organized these folks really are. These are professionals who are making billions of dollars manipulating a lot of different variables.

So we need to raise our game. I do think that is achievable, particularly if we recognize that the basics matter, and that key technologies are available than can make a big difference.”

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 435,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains, and services that span the security lifecycle, Accenture protects organizations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us **@AccentureSecure** on Twitter or visit the Accenture Security **blog**.