accenture

HOLDING FIRM

The state of cyber resilience in banking and capital markets

Accenture State of Cyber Resilience in Banking and Capital Markets

Contents

01

Introduction

Accenture's 2019 edition of the "State of Cyber Resilience" report has found that banking and capital markets (CM) firms have made great strides when it comes to not only preventing security attacks but also bouncing back from breaches quickly. One issue they face, though, is that there is a definite "yes, but..." quality to much of the good news.

Direct attacks are down, but indirect attacks are a growing concern.

For example, direct cybersecurity attacks on banking/CM firms are down 2 percent, and actual breaches are 25 percent lower than in the 2018 survey. This is, in part, a testament to their recent success and their security investments. Cyber criminals look for the easiest way available to break into systems. Banks and CM institutions have become quite challenging to penetrate, so the "bad guys" have gone elsewhere. Over the last year among the global cyber resilience survey respondents, an average of 17 attempted breaches of banking institutions' security defenses succeeded (23 for capital markets), while the numbers are larger in industries such as consumer goods (28), healthcare providers (24) and insurance (31).

On the other hand, criminals are having increasing success breaking into banks'/CM firm's systems indirectly—via the broader ecosystem that includes vendors and other third parties in the value chain. Almost 40 percent of breaches now come through the indirect route. These exposures take the form of things like injection of malicious code to a vendor's site, downloaded open-source libraries or a vendor's misconfigured server.

On average, cybersecurity programs actively protect only about 60 percent of an organization's business ecosystem. This is particularly difficult to address as companies are increasingly relying on a remote workforce. It is challenging to monitor such a workforce—especially one located across multiple companies—to check that everyone is compliant in terms of things like encrypting Wi-Fi, changing passwords regularly and staying vigilant about phishing attacks and other threats.

Banking and capital markets firms experienced fewer breaches, but are not recovering quickly enough from successful ones.

The progress made by banking/CM firms in cybersecurity can be seen in the fact that surveyed institutions as a whole experienced fewer security breaches last year (163) than the cross-industry leaders (239). On the other hand, financial institutions are lagging in areas such as:

33%

Time to detect a breach:
88 percent of cross-industry leaders discover a breach in less than a day, but only one-third of banking/CM institutions can say the same.

44%

Ability to remediate a breach within 15 days:
96 percent of leaders vs. 44 percent of banks/CM firms.

32%

Breaches with no material effect (a breach notification was required, but little or no damage was experienced):
True for 58 percent of leaders, but only 32 percent for banking/CM.

Investments are up, but firms worry that, over time, they won't be able to keep pace.

Finally, firms are investing in cybersecurity at higher levels according to our cyber resilience survey. About one-third of banking institutions spend from 40 to 60 percent of their cybersecurity budget on advanced technologies (e.g., artificial intelligence, machine learning and robotic process automation), up 9 points from three years ago. Capital markets firms are investing even more aggressively: 47 percent are spending between 40 and 60 percent of their budget on advanced technology, up from only 17 percent three years ago.

But there is a certain resignation, if not futility, that one senses about how much high-end cyber protection costs, and what it is expected to cost in the future. Fifty-six percent of banking/CM respondents report that costs for cybersecurity protection have grown over the past two years, and about one in five say that those increases were more than 25 percent. Overall, 65 percent of banking/CM institutions indicate that staying ahead of attackers is a constant battle and that the cost is ultimately unsustainable.

02

What cybersecurity leaders are doing differently

02 WHAT CYBERSECURITY LEADERS ARE DOING DIFFERENTLY

In the midst of some resignation about cybersecurity, our analysis also kindles hope for companies in that some of them are getting far better results than their peers, and their strategies and actions may inspire others. Detailed modeling of cybersecurity performance has identified two distinct groups among respondents.

The first is an elite group—15 percent of the banking and capital markets firms surveyed—that have significantly higher levels of cybersecurity performance compared to their industry peers. These organizations set the bar for innovation and show better security results. The second group forms the vast majority of our sample—75 percent—who are average performers.

The leaders exceed the capabilities of the average group in four areas in particular:

4x

Stopping more attacks:
A nearly fourfold advantage in preventing targeted cyber attacks.

4x

Finding breaches faster:
Four times faster at detecting a cyber breach.

3x

Fix breaches faster:
An almost threefold advantage in speed of remediation.

2x

Reduce breach impact:
Twice as effective at containing the damage from a successful attack.

02 WHAT CYBERSECURITY LEADERS ARE DOING DIFFERENTLY

Moving closer to a leadership position in cybersecurity can begin to address some concerns about rising costs. Our research found that the current average cost per attack for average performers was $380,000 per incident. If they could perform more effectively—that is, attain a leader's level of performance in detecting attacks and fixing breaches—our detailed modeling finds that they could reduce the cost per attack by 72 percent. This is a potential savings of $273,000 per security breach, reducing the average cost to $107,000. For these performers, who experience an average of 22 incidents per year, this equates to $6 million in annual savings.[1]

A key point to highlight in these numbers is speed. Rapidly spotting and containing breaches is the only hope for consistent and long-term resilience. Breaches are a given, but cybersecurity leaders are fast responders. They can find and stop breaches before significant damage is done. They spot anomalies, trigger an investigation and eradicate the threat. Non-leaders, by contrast, over-spend on defense and under-spend on offense—in this case, meaning not enough time building fast, sophisticated detection-and-response capabilities.

The current average cost per attack for average performers was

$380,000

per incident.

03

The challenge of indirect attacks

It is no exaggeration to say that a modern business cannot compete without relying on an extended network of vendors and other third parties.

In fact, a survey-based study among IT professionals found that the average corporate network is accessed by 89 vendors every week.[2] This ecosystem is likely to grow in scale and importance over time. The same study found that 71 percent of respondents expected their companies to become more reliant on third parties in the next two years.[3]

Other research found a steep increase in incidents involving companies that handle sensitive data for their clients. The total number of these third-party breaches was 368 in 2019, up from 328 in 2018 and 273 in 2017—a 35 percent increase in two years.[4]

There are enormous challenges in managing third-party cyber risks. Large volumes of data can overwhelm the teams responsible for managing compliance. The complexities of global supply chains, including the regulatory demands of various regions or countries, add to the strain. The nimbleness of small subsidiaries or suppliers can be hamstrung by the central security requirements of the parent.

04

Choosing the right technologies

A dizzying variety of technologies are available in the cybersecurity area. Yet, leaders know which of those technologies is best positioned to help them attain a broader level of cybersecurity effectiveness. Our study found that leaders highlight three technologies in particular:

Next-Generation Firewall (NGF)

Security Orchestration Automation and Response (SOAR)

Privileged Access Management (PAM)

The use of these technologies helps to explain how leaders are able to more quickly shut down a cyberattack, thereby limiting the damage. Next-generation firewalls help banks segment their network and prevent a breach from spreading too far beyond the initial machine that was compromised. SOAR allows very rapid responses to routine incidents such as malware on a user's computer. These types of routine issues can overwhelm security teams, leaving them with no time to search for and respond to the real adversaries.

A well implemented PAM solution cuts the attack chain at the point where the adversary tries to escalate their privileges. Each time a privileged account is used, a PAM solution requires there to be a ticket (from BMC Remedy™, ServiceNow, Inc. or a similar system). The ticket allows the administrator temporary access to the privileged account. It logs them into the system where they can make the required changes. Then it records the whole session, logs them out afterwards and changes the passwords that were used. It is password-safe for the most sensitive corporate accounts coupled with auditing and controls. When properly implemented it is very difficult for attackers to get what they want.

05

Do you want to be a cybersecurity leader?

That may appear at first to be an odd question (who doesn't want to be a leader?). However, some banking and capital markets firms might not be attracted to a leadership position because they associate it with being difficult and expensive. They might believe that they don't need to be as good as the very top echelon of firms, but rather just as good as the bank up the street.

However, a better way to think of "leadership" in this area is companies that "lead the way." Leaders are pathfinders. They don't necessarily spend the most amount of money. (In fact, over a 10-year period, they might actually spend less.) Instead, they spend it wisely and efficiently, and in a balanced way. They invest equal amounts on automation technologies and on detection-and-response rather than all of it on perimeter defense—something that our survey respondents said they'd overinvested in. So, it doesn't mean they buy the most expensive technologies that keep out the most sophisticated adversaries. It means they have a detection capability so they can spot things and eradicate them quickly. On that basis, we believe it is essential that you "follow the leaders," because any other path is ultimately cost-prohibitive and unsustainable.

Some banking and capital markets firms might not be attracted to a leadership position because they associate it with being difficult and expensive.

More specifically, cybersecurity leaders in banking and capital markets tend to:

Prioritize speed

According to our State of Cyber Resilience survey, leaders invest with an eye on improving operational speed. The top-three measures of cybersecurity effectiveness named by leaders all emphasize speed: how quickly they can detect a security breach, how quickly they can respond, and how quickly they can get operations back to normal. Beyond these priorities, leaders also measure the effectiveness of their resiliency (how quickly they recover from a breach) and their precision (improving the accuracy of locating cyber incidents).

Scale more

The rate at which surveyed organizations scale investments across their business has a significant impact on their ability to defend against attacks. The leaders best at scaling technologies—defined as 50 percent or more tools moving from pilot to full-scale deployment—perform four times better than the average performers.

The ability to scale is an important factor in the reach of security programs. The cybersecurity programs for those that are best at scaling actively protect three-quarters of all key assets in the organization according to our survey. Average performers cover only one-half of their key assets. It is a little surprising that 86 percent of leaders agreed that new cybersecurity tools are increasing cybersecurity coverage for their organizations.

Train more

The speed with which organizations in our survey find security breaches is faster for those who provide higher levels of security-related training. Across the global sample, those who were top performers in terms of training found 52 percent of security breaches in less than 24 hours, compared with only 32 percent for average performers. Time to remediate a security breach is also improved by better training. For the leaders in providing training, 65 percent of all security breaches are remediated within 15 days, compared to 36 percent of non-leaders.

Collaborate more

The organizations best at collaborating—the ones using more than five methods to bring together their strategic vendors and collaborators, the security community, cybersecurity consortiums, and an internal task force to increase understanding of cybersecurity threats—are twice as successful as others at defending against attacks. Organizations that collaborate more have a breach ratio of 6 percent versus an average of 13 percent for the rest.

Although banking and capital markets firms cannot change their risk environment, they can change what is in their sphere of control. It's important to take an "art of the possible" approach to cyber resilience: Know what's currently possible to manage and what isn't and prioritize investments to increase your sphere of control wherever possible.

06

Immediate actions and takeaways

Certainly, the biggest warning flag raised in this latest edition of the "State of Cyber Resilience" report from Accenture is the growing threats from indirect attacks—those made through vulnerabilities in the defenses of vendors, partners or subsidiaries.

The answer to this problem is fairly easy to explain, though much harder to implement and manage over the long term. It is to put in place the policies, governance and enforcement such that any third party connected to your network requires the same security standards that you do. Otherwise you've got to treat them completely at arm's length. If you do not follow this policy, your network is only as secure as the least secure entity connected to you, and all of your security spending might be going to waste.

When we turn to the issue of subsidiaries, we see the problem in especially stark relief. Companies may presume that they are treating those entities as a separate company, but in fact electronic trust is most likely fully established between them. Emails from subsidiaries, for example, are usually not marked "external." That means that a security compromise at the subsidiary gives an attacker a perfect platform to send phishing emails to the parent company, too. Soon, the parent's network is compromised, as well.

Given finite security resources, there is value in a data-driven, business-focused approach to securing the enterprise ecosystem. This may mean using threat intelligence reports to risk-prioritize which vendors are in need of better security solutions. A managed security services approach can help an organization keep vendors or subsidiaries at arms-length, where they are not connected to the parent companies' systems, including its security apparatus. This approach can help tackle issues at a larger scale and with a wider scope, without burdening the corporate security department. By collaborating more broadly with others with the common goal of securing the enterprise and its ecosystem, organizations can help themselves while also helping smaller vendors, allies and partners to beat cybercrime.

Meeting your cyber resilience challenges with Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we allow clients to innovate safely, build cyber resilience and grow with confidence.

Follow us on Twitter @AccentureSecure
or visit us at accenture.com/security

About the authors

Chris Thompson

Chris Thompson is a Senior Managing Director, based in New York. He leads the Accenture Financial Services Security and Resilience practice. The Security and Resilience practice helps clients manage cyber risk: the subversion of information risk controls for the agenda of the perpetrator. The practice unifies security, operational risk, fraud and financial crime and provides end-to-end services across strategy, simulated attacks, consulting and managed services delivery. Chris has nearly 30 years of experience with large-scale change programs, working with some of the world's leading retail, commercial and investment banks.

Valerie Abend

Valerie Abend is a Managing Director, Global Banking Security Lead with Accenture Security. With over two decades of experience spearheading financial services sector-wide and enterprise-wide security and resilience programs, Valerie is currently focused on advising C-suite executives on how to manage cyber risk to drive new business strategies and remain resilient in the face of rapidly evolving threats and heightened regulatory expectations. She is also the Chair of the Accenture Cybersecurity Forum Women's Council, which facilitates information sharing and fosters advancement of women in the security space.

Andrea Agosti

Andrea Agosti is a Managing Director, European Financial Services Lead with Accenture Security. He has over 20 years of experience in the areas of IT risk, security strategy, cybersecurity, business resilience, financial crime and cyber regulations for financial services. In Andrea's current role he helps financial services organizations and their executives in Europe strengthen their security capabilities and functions and build a security lifecycle from the inside out to respond to current needs and future challenges.

References

1. "Accenture Third Annual State of Cyber Resilience," January 2020. Access at: https://www.accenture.com/us-en/insights/security/invest-cyber-resilience
2. "Vendor Vulnerability: How to Prevent the Security Risk of Third-Party Suppliers," Bomgar, 2016. Access at: https://beyondtrust-bomgar12.netdna-ssl.com/assets/documents/Bomgar-Vendor-Vulnerability-Index-2016.pdf
3. Ibid.
4. "Third-Party Breaches—and the Number of Records Exposed—Increased Sharply in 2019," DarkReading, February 12, 2020. Access at: https://www.darkreading.com/attacks-breaches/third-party-breaches---and-the-number-of-records-exposed---increased-sharply-in-2019/d/d-id/1337037
5. "Vendor Vulnerability: How to Prevent the Security Risk of Third-Party Suppliers," Bomgar, 2016. Access at: https://beyondtrust-bomgar12.netdna-ssl.com/assets/documents/Bomgar-Vendor-Vulnerability-Index-2016.pdf

Stay connected

Accenture Finance and Risk
www.accenture.com/us-en/services/financial-services/finance-risk

Finance and Risk Blog
financeandriskblog.accenture.com

Connect With Us
www.linkedin.com/showcase/16183502

Follow Us
www.twitter.com/AccentureFSRisk

About Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries—powered by the world's largest network of Advanced Technology and Intelligent Operations centers. With 513,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at **www.accenture.com**