Think banking cybersecurity is just a technology issue?

Think again.

By Stéphane Geyres and Michael Orozco
Over each of the next four years, the cost of a cybersecurity breach will increase 100 percent annually.¹ Blame it on increasingly digitized environments and an Internet of Things that is fast creating a webbed infrastructure spanning multiple organizations, business services and data sources. The “simple” breach has gone the way of the analog phone—toward extinction.

Accenture research² shows 82 percent of risk management executives in the financial industry see emerging risks in the cyber realm account for more of the chief risk officer’s (CRO) time than ever before. As attacks become more sophisticated and frequency increases, financial institutions are in the crosshairs.

Despite significant cybersecurity spending over the past several years, many companies are still as exposed as they were before that spend. The Threat Gap—the gap that exists between investments in technology, people and processes to mitigate cybersecurity emerging threat vulnerabilities—continues to widen.

The reasons for that continued exposure vary, but they include a push toward digitalization without the accompanying shift in cybersecurity focus. With each digital door a financial institution opens to better serve clients (mobility, cloud, etc.), new vulnerabilities too often arise. Yet, digitalization is necessary to meet consumer demand for simplified 24/7 access.

To address the changing environment, banks need to take a broader, intelligence-based approach to cybersecurity, factoring in new threats such as geopolitical climate, third-party risk and exposed insiders. In addition, for success over time, cybersecurity needs to be baked into the business—products, services and digital investments enabling technology, processes and people—to help drive growth and profitability and foster sustainable resilience. A failure to invest will put your organization’s long-term competitiveness at risk.
Ignore the Threat Gap at your own peril

Ignore the Threat Gap and a breach becomes a sure thing. The wiser course of action is to shift from a focus on known controls and known threats to integrating intelligence, strategy and planning to mitigate risk over time. As Don Anderson, senior vice president and CIO at the Boston Fed, said at his organization’s 2016 Cybersecurity Conference: “The bad guys have technology too. Now is the time to disrupt ourselves.”

Most banks and capital market firms are not investing in this course of action as they should. In 2016, 75 percent of banking executives expect to invest in hardened devices and encryption, 66 percent in better protection around systems, but only 20 percent in improved intelligence gathering and assessment. The first two actions will not by themselves stop breaches. An intelligence-focused approach will be required to create a comprehensive strategy. You cannot defend against what you do not know. The variables continue to multiply: Who is the most likely adversary—a political activist or a criminal enterprise? What does the attack target—theft of financial positions or sensitive client data?

True cybersecurity is a combination of defense, resilience and assurance. It is not simply purchasing the latest cybersecurity product. It requires a new mindset as well as a new skill set.

Defense
A good defense means a breach is detected immediately, with the appropriate real-time reaction. That reaction should spark a chain of events to contain the breach and protect the organization from further harm. Common defensive measures include technology to monitor and detect intrusions or abnormal behavior. Data encryption and network segmentation help reduce the usefulness of any stolen information. By separating systems, data and applications, organizations better contain threats. Most companies have a line of defense addressing malware and traditional hacking. What they lack is defense that covers newer threats such as third-party vulnerabilities, insiders or geopolitical risk.

In 2016, of banking executives...

75% expect to invest in hardened devices and encryption

66% in better protection around systems

But only 20% in improved intelligence gathering and assessment.
Resilience

Resilience limits the negative impact of a breach. The best resilience allows enterprises a quick return to normal operations with the least impact to customers and the bottom line. Organizations need to be able to withstand cybersecurity attacks while maintaining operational and service levels. Resilience builds upon defense with actions such as: proactive controls, crisis response protocol testing, cybersecurity readiness assessments, and hacking tests. With many organizations moving to a platform-based ecosystem model, resilience becomes more important than ever. As devices and institutions become more linked, breaches to any one member of an ecosystem can put the entire membership of that ecosystem at risk. Three out of every four banking executives surveyed see their organization as lacking in a strong cybersecurity defense across their ecosystem, which means most banks do not have effective resilience in this area.

Assurance

Assurance means defense and resilience are incorporated into day-to-day business. Organizations should conduct frequent tests of their cyber defense; track adherence to security procedures; and monitor employee cyber education, risk habits and behavior. Doing so gives them a basis for an assurance-balanced scorecard. We also recommend developing a maturity model to help identify strengths and areas for improvement. Teams then can remediate to strengthen the organization’s enterprise cybersecurity posture. Assurance, ultimately, involves baking security into the DNA of your business—into every new product and service—not as an afterthought, but as a matter of course.
Most banking and capital markets executives view cybersecurity risks as stemming from a limited set of external sources, such as criminal elements. With that view, they are missing key threats from geopolitical risk, insider threats, third parties, social media and other areas.

Recent geopolitical targets range from South Korean banks to Spanish renewable energy companies, and from risk-hedging models to cargo in international waters. As the types and sophistication of cyberattacks stemming from geopolitical unrest increase, so should the intelligence gathering in this sector by banks and capital market firms in all areas. Attacks are not simply confined to areas of high geopolitical instability, but rather stem from those areas and affect more stable economies and business around the globe. Executives are still somewhat behind in their thinking on this issue, as only one-third view geopolitical risk as a cybersecurity threat.

Third-party risk also plays a larger role, as companies move to the cloud, housing data on third-party servers. Partners’ risk becomes yours. Additionally, as ecosystems grow to be the primary method of conducting business, risk is spread over a broader playing field. Malicious parties who breach one node of an ecosystem stand to gain control over far more data than they did in years past, if all partners are not duly diligent. Despite this fact, only 31 percent of executives plan to invest significantly in improving unified cybersecurity strategies across the ecosystem.

Most banking and capital markets executives view cybersecurity risks as stemming from a limited set of external sources, such as criminal elements.

With that view, they are missing key threats.
Social media sites increase exposure not only because of the greater chances that they deliver malicious content but also because of what employees may disclose that could compromise company security. Add to that the potential for fraudulent tweets and a company’s stock price could be at risk. For instance, a tweeter that appeared to be Russian Interior Minister Vladimir Kolokoltsev (but was not) falsely claimed that Syrian President Bashar al-Assad had been killed. Between 10:15 a.m. and 10:45 a.m. the same day, futures for light, sweet crude rose from $90.82 to $91.99 a barrel on the New York Mercantile Exchange before traders were informed the news was false.\(^5\)

Insider threats are on the rise, as employees go rogue for monetary gain or are coerced to avoid harm to their families. Schemes range from kidnapping, to corporate espionage, to disgruntled employees who want retribution during a period of layoffs, to an executive who is simply careless with a password. Regardless of the situation, banking executives do not take this threat seriously enough. More than two-thirds of them see individual criminals/organized crime as threats; only 33 percent consider penetration of executive protection as such.
Cybersecurity is not an IT problem. It’s a C-suite problem.

Anything that can cripple a business in a matter of minutes is a C-suite problem. Cybersecurity belongs at the decision-making table as new products, services, processes and people are brought on board. The numbers show banks and capital markets firms have work to do in this area: more than two-thirds of banking executives do not believe business unit and functional cybersecurity strategies are aligned with leadership and across the organization.

The cost of not investing properly and in accordance with the firm’s risk profile rises exponentially when a cybersecurity event occurs. It is no longer a question of if a firm will be attacked, but rather when—and how much the attack will impact the business. Paying for cybersecurity is sometimes seen as a grudge purchase, similar to purchasing insurance. We anticipate higher investment as corporate boards become more aware and active in questioning whether their organizations are truly secure.

Leaders need to integrate cybersecurity into the business, from training new employees in appropriate procedures to building security into a new product launch. Banks have some distance to travel in this regard—less than half of banking executives surveyed feel cybersecurity assessment and planning is effectively integrated with product development. Security teams should be part of core product teams.
Taking cybersecurity beyond technology

Organizations who want to close the Threat Gap will take immediate action before it widens. Among the smart moves are:

**Adjusting the organizational chart.**
Broaden cybersecurity efforts from the chief information security officer to include the COO, CRO, CEO and the board. Just as these stakeholders vet strategic business decisions, they should also assess threats and major investments that stand to compromise your business.

**Making cybersecurity a reported expectation on all projects.**
Ensure it is integrated into designs, architecture, user acceptance, processes and people from day one.

**Broadening your scope.**
If you are not considering the expanded spectrum of emerging threats, your Threat Gap is a gaping chasm. An intelligence-based approach to cybersecurity is crucial.

Barring prescience, a solid plan to gather intelligence and address threats from a growing number of sources is the best defense over time.
Photography may also be incorporated as a background with the red, black and white color scheme remaining dominant.

Turn off NOTES in Layers menu to eliminate these notes.

Copyright © 2015 Accenture. All rights reserved. Accenture, its logo, and High Performance Delivered are trademarks of Accenture.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

References
4. This and all subsequent statistics are from the Accenture Cybersecurity in Banking and Capital Markets Study, 2016, unless otherwise noted.

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 approximately 373,000 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 Strategy
Accenture Strategy operates at the intersection of business and technology. We bring together our capabilities in business, technology, operations and function strategy to help our clients envision and execute industry-specific strategies that support enterprise-wide transformation. Our focus on issues related to digital disruption, competitiveness, global operating models, talent and leadership helps drive both efficiencies and growth. For more information, follow @AccentureStrat or visit www.accenture.com/strategy.