Banking Risk Landscape: Is Your Security Solution A Secure Solution?

Five Critical Questions Bank Security and IT Leaders Need to Be Ready to Answer

Organizations across the world face a new risk paradigm: one that encompasses cyber and physical threats. We've heard the stories associated with ATM skimming, identity theft, data breaches, scams, and phishing. Large financial services organizations are often the victim of hackers looking to steal corporate information and transactional data or funds, and criminals continue to become more sophisticated in their approach.

Additionally, cyber threats have taken a front seat in the lineup of primary risks facing financial institutions today. And it is no surprise why: According to Cybersecurity Ventures, the amount of money taken in cyber heists, both in banking and elsewhere, was estimated at $3 trillion overall for 2015, and this substantial amount is expected to double by 2021.

The fact that cyberattacks are becoming more prevalent isn't the only issue; they're also becoming more complex and therefore harder to address. And although the convenient interconnectivity of the Internet of Things (IoT) creates many advantages for financial institutions, with that also comes an increased risk to dangerous threats. In today's environment, banks, credit unions, and financial organizations of all types are primary targets for hackers. But it's not just the monetary loss that these businesses need to be concerned about — there is also a threat to the brand, customer trust, and employee safety.

All of these challenges and complexities open the door to new conversations and risks. Here are the top five critical questions today's bank leaders need to be ready to answer.

1: Is it best to collaborate to mitigate these threats effectively?

Over the last decade, the emergence of the Internet of Things (IoT) and a demand for more mobile capabilities has changed the way people and businesses connect. But as the need for connectivity increases, so too does the need for increased security for physical assets, networks, and valuable corporate data. As a result, a dialogue between IT and physical security is necessary to help leaders gain a greater knowledge of how to best collaborate to ensure complete protection. Leaders must communicate closely to drive strategies that help identify vulnerabilities in a more proactive manner. The result of these conversations: a truly comprehensive approach to security intelligence.

2: How can I pinpoint the important data necessary to address cyber threats proactively?

To maintain a high level of security and ensure business continuity around the globe, companies seek solutions that help predict and identify threats in real time. But often, there are too many alerts generated by too many systems, and none of this raw data is actionable. Linking cyber and physical security together transforms alerts into actionable intelligence, which helps users connect the pieces of any situation and present a unified risk scenario to the appropriate analysts and operators. By capturing and analyzing data in real time, enterprise organizations gain a visual representation of risks across the business while accessing information related to the most critical events happening at any given time. Not only does this unified process enable a higher and more proactive level of protection, but it also helps facilitate a plan of action based within a common, unified security operations center. communicate closely to drive strategies that help identify vulnerabilities in a more proactive manner. The result of these conversations: a truly comprehensive approach to security intelligence.

3: Can we "talk" cybersecurity?

Security leaders in banks need to feel prepared by staying updated, looking at common vulnerabilities, understanding the malware and challenges, and testing the environment. And collaboration is key to mitigation: Traditional security and fraud teams must work in conjunction with cyber teams to effectively handle all aspects of a cyberattack. Additionally, CISOs need to "sell" cybersecurity to CEOs and the board by outlining the importance of protection through emphasizing the impact of a potential cyberattack on the business. Ensure you can verbally address the most critical risks to your senior leadership, including recent botnets, scams, and cyber gangs, to receive the support (and budget) you need to address these threats head on.

4: Is my system secure?

It is critical that you are knowledgeable about the steps you can take to protect your security and network infrastructure from cyberattacks. Changing default passwords should be a first step, as some scams target devices with hard-coded factory defaults. Ensure software and firmware is up to date because updates often include fixes for potential vulnerabilities. These updates keep your devices and network more secure and increase overall system uptime. A firewall is useful to prevent hackers and unauthorized programs from accessing the critical business information and resources on internal networks and computers. Also, minimize potential risk by closing network ports and disabling services you don't need. With all of these instances, it is best to work closely with your integrator partner and chosen vendor to ensure that your system is as secure as it can possibly be.critical risks to your senior leadership, including recent botnets, scams, and cyber gangs, to receive the support (and budget) you need to address these threats head on.

5: What solutions are best to help mitigate risks?

Technology is a great force multiplier. Security — both cyber and physical solutions — helps secure an entire branch footprint, alleviates risk, ensures operational compliance, and improves fraud investigations. Verint's comprehensive and robust surveillance systems can provide organizations with intelligence and unprecedented protection from fraud, all while enhancing the customer experience.

At Verint, we practice the same concepts outlined here, combining physical and cyber security efforts to realize comprehensive risk intelligence. By bringing various leaders, departments, technologies and strategies together, we can more effectively identify threats, develop trends and quickly access important data to ensure security and safety goals are realized. Our goal is to help financial organizations achieve the same.

Verint. Powering Actionable Intelligence®

Verint® Systems Inc. (NASDAQ: VRNT) is a global leader in Actionable Intelligence® solutions for customer engagement optimization, security intelligence, and fraud, risk and compliance. Today, more than 10,000 organizations in over 180 countries use Verint solutions to improve enterprise performance and make the world a safer place. Learn more at www.verint.com.

Americas

✉ info@verint.com

☎ 1-800-4VERINT

Europe, Middle East & Africa

✉ marketing.emea@verint.com

☎ +44(0) 1932 839500

Asia Pacific

✉ marketing.apac@verint.com

☎ +(852) 2797 5678

verint.com   twitter.com/verint   facebook.com/verint   blog.verint.com