Financial services cybersecurity defenses

Fighting back and the inoculation of an industry

IBM

Executive summary

The commoditization of hardware and software is driving the use of technology deeper into society - but the abundance of technology capabilities cuts both ways. The sophistication of cybersecurity has been evolving for decades - easily keeping pace with the growth of technology in the digital age. For the financial services sector, with a heavy reliance on technology, this has come to mean that we expect to hear about a new cyberattack on an almost daily basis. The constant adoption of new technology into the financial services sector to enhance banking products like—the ATM, credit cards, mobile banking and payment platforms as well as improving staff productivity by leveraging remote access, mobile and cloud applications—present many opportunities for cybercrime. The latest cyber fraud incidents around SWIFT-connected payments systems are just the most recent of these attacks, and serve as a wake-up call to many.

This paper examines some of the critical security issues facing the financial services industry. It addresses how security, when implemented as an immune system, can help prevent these attacks by enabling companies to identify and rapidly respond.

Combating sophisticated adversaries requires powerful, proactive counter-fraud and security programs using innovative technologies to combat cybercrime. For instance, cognitive computing is helping financial institutions analyze mountains of previously unused data, discern suspect relationships, and identify patterns and outliers that are indicators of cybersecurity threats. Blockchain technology is also now in use to reinforce Know your Customer (KYC) compliance with other new use cases being created to address similar needs. In addition, advances in access management makes access fast and simple for authorized users to access the right applications and the right data while effectively blocking unauthorized users.

Cyberthreats will continue to evolve in lock step with advances in technology. It is critical then, to use those same technological advances while simultaneously fighting against information silos - both are essential weapons in the fight. Technologies such as blockchain and cognitive computing, and expansion of information sharing are at the forefront in combatting today's cyberattacks.

Moving to an integrated approach

Many large banking and financial services firms admit that traditional security practices have become unsustainable. As the threat landscape grew, some companies responded by deploying a new tool to address each new risk. IBM research found one company had deployed 85 different security tools from 45 vendors.[1] Costly and complex, these fragmented security capabilities do not provide the visibility and coordination needed to stop today's advanced attacks. Moreover, the skills, expertise and number of professionals needed to keep up with a constant stream of new threats is not feasible. According to industry reports, the global shortage of IT security experts tops 1 million.[2] As new risks emerge, the environment will grow more complex and the skills gap will widen. Many security teams are simply operating in the dark, as criminals grow more emboldened.

Combating today's steady stream of cyberattacks requires a security ecosystem integrating all the security tools and programs that prevents, detects and responds to cyberattacks. Consider the integrated security system as similar to how our immune system protects us from germs. There are multiple levels of defense, each performing a different task to keep us healthy. An integrated security system works in the same manner. There are a variety of approaches that are taken to keep systems "healthy" and productive. See figure 1.

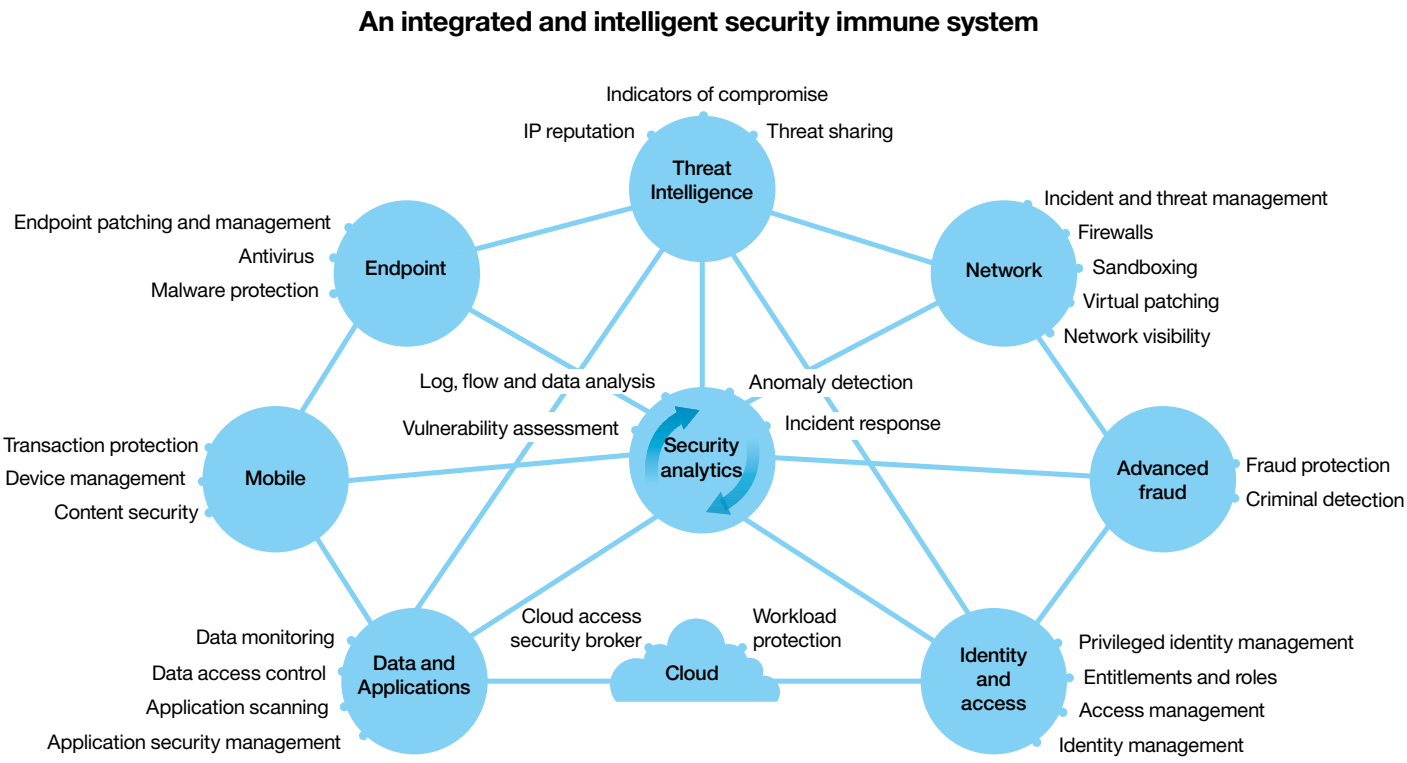

Figure 1. Security as an immune system

The core of the security immune system is built on security analytics. Similar to how a body collectively responds to a cold or virus, firms must centralize the collection of data from key areas in the enterprise to better understand what is happening inside the institution. And when these key areas begin talking to each other, the system becomes integrated, making the exchange of critical data simpler and more effective. For financial institutions, it's not a complete immune system until domains can interact and communicate with one another across hybrid IT environments in the same manner; extending beyond your firm's walls and across the entire ecosystem. Many financial institutions have already started this journey building Fusion Centers to foster domain experts across the enterprise to better interact and communicate.

Correlation and behavioral analytical tools can then help establish ongoing monitoring to detect threats. Cognitive technology will collect threat intelligence from sources such as blogs, social media, and security-themed websites to better understand the latest threats impacting society, the banking industry, and their peers. Enterprises can use this previously untapped threat intelligence to distill early warning indicators to proactively implement changes into their security controls and prevent future attacks.

When an attack happens, a rapid response must be employed to contain the incident from spreading, eradicate the infection from the organization and return to normal business operations. Enterprises wishing to recover rapidly must have:

- Well documented and distributed incident response plans
- Training that includes attack simulation exercises and incident response procedure testing
- Active threat hunting
- Procedures for continuous threat monitoring of the environment.

Security intelligence and operations

Security intelligence uses behavioral analytics to identify deviations from regular patterns—changes in network traffic, end point activity and more—that indicate possible threats. In a security intelligence infrastructure, analytics are applied to massive amounts of information in an effort to understand the data. By determining which deviations are meaningful, security intelligence can help detect compromises faster, and reduce false positives to save time, resources and improve the customer's experience. An integrated security immune system uses the lessons learned from data analysis by applying security changes to the appropriate security control points within the operating environment that prevents and detects cyberattacks. With analytics at the core, the immune system approach delivers a level of maturity that no single security solution can provide on its own.

At the heart of a security intelligence capability is the security information and event management (SIEM) system, the realization of the integrated approach discussed earlier. The SIEM system combines the security information from all the security tools into a centralized repository where enterprises can analyze this disparate data from a single point of view to spot trends and detect abnormal patterns.

A finance company implements IBM SIEM solution to better manage its security infrastructure

A finance company turned to IBM when they realized their existing solutions were insufficient to combat growing internal and external security threats. IBM identified weaknesses in administrative, operational and technical security controls as compared to industry standards and implemented the Q-Radar® SIEM solution to address these issues. With the implementation of this solution, the client has been able to efficiently manage security infrastructure compliance, optimize TCO for security operations and establish effective security policy governance to gain focus on management of high-risk areas.

Combatting cybercrime through innovation

To analyze potential threats as they arise, data analysts and investigation teams must gather, analyze, and put into context endless amounts of data. With more than 2.5 quintillion bytes of data[3] generated every day, this is a near-impossible task. While some of the data is structured and can be consumed and analyzed by machines, much of it is unstructured data that requires the abilities of the human brain to correlate and contextualize information. This unstructured data often proves most valuable in detecting and stopping threats before they cause harm.

Unfortunately, with the speed and scale of data related to cybercrime threats in today's global financial sector, it has become unrealistic to stay abreast of the thousands of threat intelligence feeds, blogs, reports, and data. For that reason and purpose, cognitive computing holds the promise that all unstructured information will be readily available to security experts.

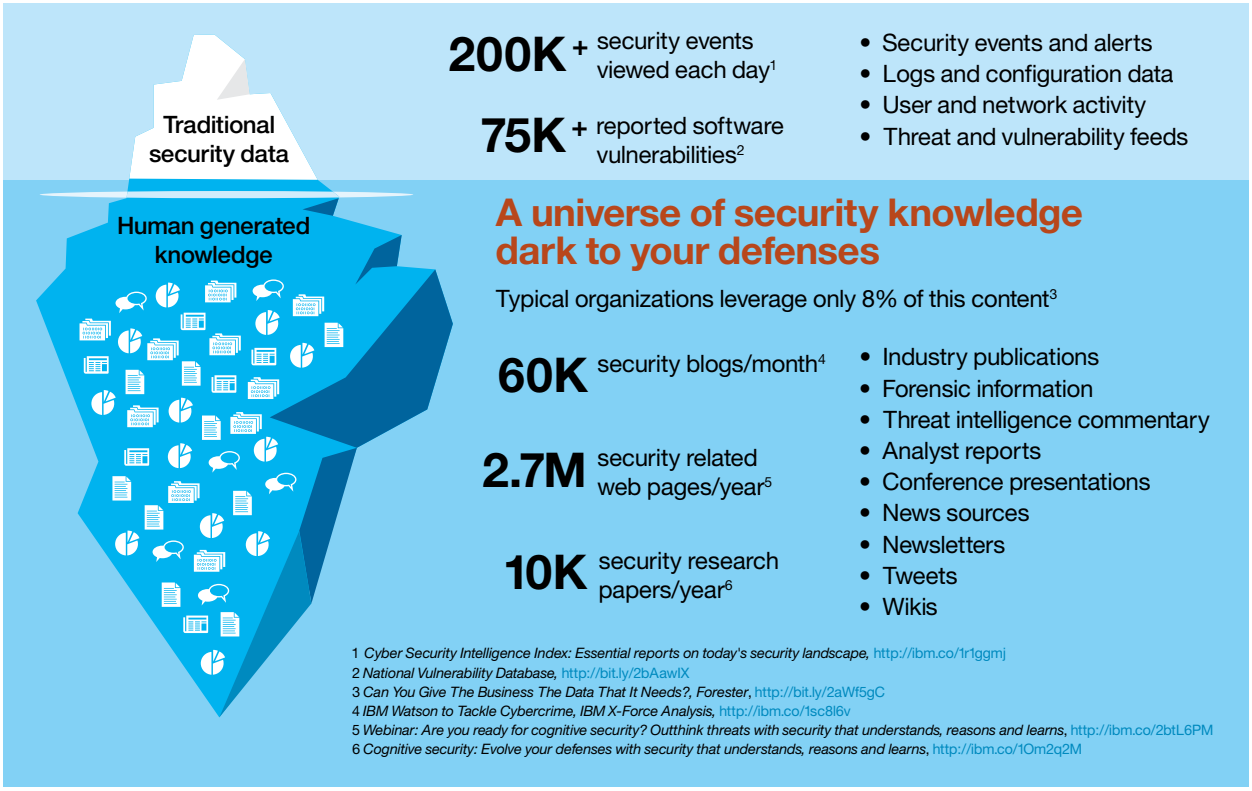

Figure 2. A universe of security knowledge dark to your defenses

Cognitive computing

For banking and financial markets, cognitive computing has arrived, and its potential to revolutionize the industry is enormous. With the power to unleash a new era of innovation and growth, cognitive systems are already helping institutions evolve beyond digital banking to further enhance the customer experience, uncover new insights and improve the quality of timely decisions.[4]

Cognitive systems are probabilistic. They are not tasked with generating narrow answers from known numerical problems, but instead are being used to develop hypotheses, reasoned arguments, and recommendations around otherwise disparate data sources. This data is often deep below the surface and normally dark to your defenses, as shown in figure 2.

Cognitive computing applies machine learning algorithms and natural language processing to make sense of vast quantities of data—both structured and unstructured—to improve data-driven discovery and decision making. While financial institutions can still derive value from analytics solutions, the addition of cognitive capabilities could help them reach new levels of value.[5]

Cognitive systems can mine data, learn the nuances of security research, discover patterns and evidence of hidden cyberattacks. It can be used to outpace security breaches by imparting insight into emerging threats and recommendations to counter them in a way that previous analytics systems could not.

Cognitive computing can help address issues such as:

- Addressing the cybersecurity skills gap
- Tapping into previously unused security intelligence data
- Reducing response time with targeted, context driven security insight

Security solutions using cognitive computing are a smarter approach to risk management. Cognitive computing is driving transformational change by harnessing not just data, but meaning, knowledge, process flows and progression of activity at a lightning-fast speed and scope. For organizations that embrace cognitive capabilities, the competitive advantage will be significant and far-reaching.

In the future, cognitive capabilities could enhance more individualized risk assessments, as well as improved risk calculations for complex, data-intensive transactions. Moreover, as future cognitive systems have access to growing amounts of historical data and analysis, recommendations on financial matters could grow in both effectiveness and scale.[6]

Blockchain

IBM is playing a central role in the development of permissioned blockchains. Having contributed more than 40,000 lines of code to the project[7], IBM is proud to be a founding member of the Linux Foundation's open-source HyperLedger Project. The project is helping to build the foundational elements of business-ready blockchain architecture with a focus on privacy, confidentiality and auditability. IBM has joined consortia that are developing industry-specific blockchain implementations and is pioneering the use of blockchain in its own operations.[8]

Blockchain's appeal is that it offers up the potential of reducing the cost of making payment transactions and has the opportunity to re-engineer how markets and the transfer of assets occur. Blockchain offers up exciting opportunities to automate business processes, reducing process timeframes, giving additional visibility into the transactions (transfer of assets) thus allowing deeper data analytics to drive out additional business value.

Computers verify each transaction with sophisticated algorithms to confirm the transfer of assets and create a historical ledger of all activity. The computers that form the network are not owned or controlled by any single entity. Participants in markets powered by blockchain have virtually real-time status of transactions, and presents an immutable transaction profile, rendering that aspect more resilient than the central authority approach to verification that is prevalent today.[9] To learn more about blockchain, visit the IBM website "What is blockchain?"[10]

The transformative powers of blockchain

In late June 2016, IBM and Crédit Mutuel Arkéa completed their first blockchain project to improve the bank's ability to verify customer identity. The result of this pilot was an operational permissioned blockchain network that provides a view of customer identity to enable compliance with Know Your Customer (KYC) requirements. This demonstrates the disruptive capabilities of blockchain technology beyond common transaction-oriented use cases. "Blockchain is a transformative agent in our operational application, as proven by this project—the first of its kind in France. This pilot offers a complete view of customers' documents across our distributed network," said Frédéric Laurent, COO Innovation & Operations, Crédit Mutuel Arkéa. "The project helped us to understand and master blockchain for other client uses. Now, we are ready to incorporate this technology in our ecosystem."[11]

Through its open source contributions and resources for blockchain software developers, IBM is advancing the science of blockchain, helping to remove complexity, and making it more accessible and open. Financial services, supply chains, IoT, risk management, digital rights management and healthcare are some of the areas that are poised for major changes using blockchain networks.[12]

Anti-money laundering and Know Your Customer

The rapid shift to alternative and faster payment requirements not only brings increased cyber and fraud risk, but is also having an impact on the regulatory demands facing financial institutions to comply with anti-money laundering (AML) and Know Your Customer (KYC) requirements. Failure to identify beneficial owners of all entities and subsidiaries, inability to detect complex money movement between customers, beneficiaries, potentially sanctioned entities or persons are indicators of a poor AML program. Inadequate AML programs for establishing and managing customer risk have resulted in damaged reputations and significant fines for institutions as evidenced by several multi-billion dollar fines imposed in the US and UK during the last 2 years.

Integrating cyber, fraud and AML data points into a cognitive computing environment has allowed IBM to help customers collect and then access all customer data more effectively. This includes both transactional, non-transactional, structured and unstructured data for a more complete understanding of a customer's "normal" behavior patterns. With the aid of Champion challenger-style modelling (See Champion challenger overview[13]) and machine learning analytics, institutions can better detect cyber driven account takeover, payment systems-related malware driven attacks, ATM compromise, transaction structuring, customer fraud, and so forth. They can then react and adapt in near real time.

Security 101

Besides Security Intelligence and Operations, several security programs are mandatory. These mandatory security programs are considered table stakes within the industry and perform the basic blocking and tackling that are required at a minimum to protect the enterprise.

Network security

Network security acts as the first line of defense protecting a company from cyberattacks. Businesses face attacks against their networks on an almost continuous basis, some of those attacks are benign like the proverbial knock on the front door but others are more serious. The defenses put in place act as part of an effective security immune system, where multiple elements work together to provide a mature network security program that is able to continuously adapt to today's advanced attacks. Failure to do so can be catastrophic. This is illustrated by a bank in Asia which had (USD) millions stolen due to lack of a firewall and second hand routers.[14] Lack of attention to basic security measures cost the bank money, but also taxed it with reputational and collateral damage because of the breach.

Healthy security programs employ the construct of "network segmentation" where staff, business as usual applications, and critical business applications—such as payment systems—are separated by their distinct networks in order to boost their ability to combat threats.

Access management, data and application security

For the financial sector, protection of client and firm data is a fundamental issue, demanding the strictest of policy adherence. An IBM study reported that the financial industry was the most targeted industry and recipient of 25 percent of all cyberattacks in 2014[15]. It remained one of the top-targeted industries in 2015.[16] Clients bank with financial institutions they trust. When that trust is broken, clients take their business elsewhere. A lapse in financial security today may result in legal and response fees, and may include regulatory fines. However, it should be no surprise that according to the 2016 Cost of Data Breach Study, the largest cost resulting from a breach is lost business. The cost of lost business, as shown in figure 3, includes abnormal turnover of customers, increased necessity for customer acquisition costs, reputation damage and diminished goodwill.

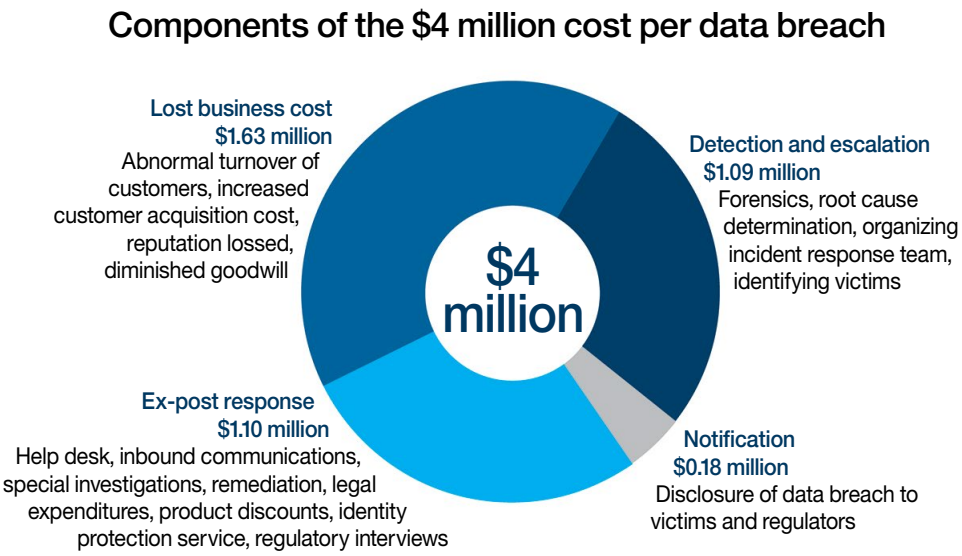

Figure 3. 2016 Ponemon Cost of Data Breach Report[17]

Security is not just about defending your infrastructure from the hackers and external threats. It also means controlling access to IT resources and data, making access fast and simple to authorized users, and effectively blocking unauthorized users. It means balancing the user experience with identity and access management (IAM) capabilities. This includes user provisioning, single sign-on, web access management, lifecycle governance, and federation. Critical systems like payment systems should be classified as a company's "crown jewels" and thus require additional controls, visibility and oversight.

An effective critical data protection strategy can help protect vital business information over the full data lifecycle—from acquisition to disposal—and across all lines of business the data touches. A critical data protection program involves five elements:

- Define: Determine security, access and exchange priorities for critical data. Define critical data specific to each element of your business
- Discover: Understand the current data security environment and infrastructure. Define your data discovery process, and perform data analysis and classification
- Baseline: Establish baselines for critical data, assessing and scoring current data security processes and controls, and performing a gap analysis and develop hypotheses
- Secure: Develop a risk remediation plan, prioritizing and validating risk remediation solutions, planning, designing and implementing critical data security solutions

People

People can be the weakest link in corporate security. Unhappy employees or disgruntled former employees with access to sensitive data represent a significant threat to corporate security. In addition, unwitting workers might inadvertently fall for phishing emails and wind up compromising corporate assets. There are regulatory policies that require financial firms to have training

and awareness programs to address this risk but to also ensure staff are aware of corporate security policies. In 2015, 60 percent of attacks were carried out by those who had insider access to organizations' systems.[18] IAM technology can be used to initiate, capture, record and manage user identities and their related access permissions automatically. This ensures that access privileges are granted according to the same policies, and individuals and services are properly authenticated, authorized and audited.

Security hygiene

Since the creation of Common Vulnerabilities and Exposures (CVE) security hygiene activities mostly involved tasks like security patching as well as system and activity monitoring. Completing these activities in an efficient, reliable and timely fashion was the hallmark of a robust security posture—at least at the technical level.

A key element in any security hygiene program is ensuring the organization has the tools to discover and maintain visibility into a company's inventory of devices, along with the ability to manage and patch the devices remotely. It is important to recognize that any device or system has the potential to harbor new threats. We need to manage our technology environments accordingly.

Security hygiene also requires people and processes in place to tune the security tools. Cyber criminals are continuously innovating on how to further advance their attack capabilities with new social engineering techniques, new tools (e.g. malware) and coming up with new ways of orchestrating attacks. If organizations do not have people and processes in place to tune their security tools, their defenses become static and eventually the cyber criminals will find a weakness to exploit.

Regional bank in North America uses IBM BigFix to reduce patch times

A large bank suffered from long software update cycles, a large number of manual patches and poor visibility into what assets were on the network. Most locations lacked IT resources so they could not effectively manage their highly distributed environment with thousands of branches and more than 50,000 endpoints. These issues also made it difficult to provide required compliance data to the security and risk management teams. The bank used IBM BigFix patch, an automated patch management tool that helps reduce patch cycle times from days and weeks to hours or minutes. The bank reduced update time from two or three weeks to two or three days for more than 50,000 endpoints on its network.

Endpoints

Endpoint security is a critical component to the security immune system and security hygiene. According to the National Vulnerability Database, there are an average of 24 new vulnerabilities published on a daily basis.[19] This number is the perfect illustration of the need for effective security hygiene. For organizations that do not keep pace with security patching, the volume of vulnerable devices in the infrastructure can create an insurmountable backlog. Attackers use the same methods to carry out cyberattacks until they no longer work; going after endpoints until they are patched, for example. With the number of vulnerabilities published daily, timely security patching is critical to the security immune system.

Cyberattacks, like the cyber heists involving SWIFT, requires an endpoint security solution that facilitates security patching. When endpoints are properly patched, the risk of malicious emails being able to deliver malware through exploitation is significantly reduced. On average, it takes 100 to 120 days to patch vulnerabilities.[20] According to a NopSec security report,

the financial services sector takes, on average, 176 days to patch vulnerabilities.[21] Beyond simply controlling access, endpoint security tools also provide capabilities such as monitoring for, and blocking risky or malicious activities.[22]

Threat intelligence sharing

In the ever-shifting landscape of cyberthreats, access to timely intelligence is critical and can protect organizations and firms against security incidents. Revisiting the immune system analogy, no one mechanism in our body is solely responsible for fending off disease. It is the combination of medication, highly trained physicians and our immune system working together that fends off the threat of disease. A firm's access to information and intelligence through sharing of that data creates a powerful treatment program for cyberthreats. Unfortunately, 68 percent of CEOs were unwilling to share cybersecurity information with outsiders[23].

Many security professionals share information informally through phone and email. Clearly, this approach is insufficient to handle the volume and velocity of cyberthreats. Leaders in global information sharing have emerged to help address these issues. One such group is the Financial Services Information Sharing & Analysis Center (FS-ISAC).[24] The FS-ISAC was created as a member-owned nonprofit entity and is the largest information sharing organization for the financial services sector with over 7000 member institutions and 12,000 portal users producing over 500 alerts a month.[25]

Responding to cybercrime

Having an incident response plan (IRP) in place can help to restore operations quickly, help protect sensitive data, systems and networks. In addition, an IRP can assist in investigating the extent and source of the breach, reducing the risk that news headlines become a distraction. Failure to implement an IRP can lead to unforeseen damage, lost productivity, bad press, client frustration, and heavy fines by regulators.

A complete IRP addresses the detection, containment, and eradication of a cyber breach. It assists in recovery of normal operations, and provides valuable follow-up analysis. When creating your plan, consider the following ideas.[26]

- Establish priorities.
- Be ready to investigate
- Have a communication plan.
- Have a containment plan.
- Analyze the incident and the effectiveness of your response to help prepare for the next event.

The IBM approach to security

IBM security solutions are built on an integrated framework that spans hardware, software and services. These capabilities are delivered through a framework defined by four domains:

- Security transformation services: Optimizing your security strategy and program with expertise and skills to address modern-day risks
- Security operations and response: Helping orchestrate your defenses through the attack lifecycle
- Information risk and protection: Keeping critical information protected
- Innovative technologies and deep analytics: Developing cutting edge cognitive and information sharing technologies, led by IBM® Watson™ can provide the tools to combat cyberthreats.

With a security team of 7,500 people, more than 12,000 customers in 133 countries and more than 3,500 security patents, IBM is an industry leader committed to helping protect the financial services industry. With an approach based on a security immune system and advanced cognitive computing, IBM can provide a pathway for growing the business while reducing the risk.

IBM Security solutions

The following solutions are a sampling of IBM security solutions. Your IBM representative or IBM Business Partner can go into detail about all of IBMs offerings in the security field.

IBM QRadar Security Intelligence Platform

The IBM QRadar Security Intelligence Platform provides an architecture for integrating SIEM, using the advanced Sense Analytics Engine to detect advanced threats. Learn more.

IBM Safer Payments

IBM Safer Payments applies machine-learning models to help detect fraud and help reduce fraudulent events. Analyzing, scoring and responding to complex fraud patterns in real time keeps the firm one-step ahead of evolving, unanticipated fraud threats. Learn more.

IBM Security App Exchange

The IBM Security App Exchange allows customers, developers and business partners to share applications, security app extensions and enhancements to IBM security products. This gives security teams collaborative tools to defend against cyberattacks. Learn more.

IBM Security Trusteer

IBM Security Trusteer® Advanced fraud protection solutions help prevent malware and phishing-driven fraud, detect account takeover attacks and fraudulent transactions, and control mobile fraud risk. Millions of users rely on Trusteer solutions to protect web applications, computers and mobile devices from online threats. Learn more.

IBM Watson for Cyber Security

In early May 2016, IBM announced Watson for Cyber Security, a new cloud-based version of the company's cognitive technology. IBM is collaborating with eight universities to greatly expand the collection of security data with which IBM has trained the cognitive system. Learn more.

IBM X-Force

IBM X-Force® monitors the latest threats including vulnerabilities, exploits and active attacks, viruses and other malware, spam, phishing, and malicious web content. X-Force also delivers security content, products, and services to help protect IBM customers:

- IBM X-Force Research and Development. Learn more.
- IBM X-Force Exchange. Learn more.
- IBM Security X-Force Threat Intelligence. Learn more.

Conclusion

Cyber threats are not new but times and techniques have changed. The lure of large financial gains has criminal groups working tirelessly to find ways to steal money from unsuspecting individuals and financial institutions.

Not every financial firm is on the same page in terms of prioritizing security. The sensitive breaches in security happening almost every week have served as notice for leaders in the financial industry to respond to the security issues they face. From eliminating the siloed information stores to technology developments such as cognitive computing and blockchain, the financial industry has begun to fight back.

For more information

To learn more about financial fraud, please contact your IBM representative or IBM Business Partner, or visit the following website: http://ibm.co/29QDqJj

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

[1] IBM client example, Get out of the silo: Disrupt the attack chain with integrated security, http://ibm.co/2aSaHjB

[2] One Million Cybersecurity Job Openings in 2016, http://bit.ly/2b4eqLK

[3] MG Siegler, Eric Schmidt: Every 2 Days We Create as Much Information as We Did Up to 2003, http://tcrn.ch/29FgZR8

[4] Breathrough banking: Your cognitive future in banking and financial markets, http://ibm.co/1HJHT56

[5] Breathrough banking: Your cognitive future in banking and financial markets, http://ibm.co/1HJHT56

[6] Breathrough banking: Your cognitive future in banking and financial markets, http://ibm.co/1HJHT56

[7] IBM Delivers Blockchain-As-A-Service for Developers; Commits to Making Blockchain Ready for Business, http://ibm.co/1MksJ8N

[8] "Blockchain: Securing the Financial Systems of the Future" http://ibm.co/23WOSlM

[9] The Blockchain: What It Is and Why It Matters, Sheel Tyle and Mohit Kaushal, http://brook.gs/2bcW9ga

[10] Learn more about blockchain at http://ibm.co/29MuPWb

[11] IBM and Crédit Mutuel Arkéa Pioneer the Use of Blockchain to Manage Customer Identity and Improve Customer Satisfaction, http://ibm.co/2aygUTH

[12] Press release, 30 Jun 2016, IBM and Crédit Mutuel Arkéa Pioneer the Use of Blockchain to Manage Customer Identity and Improve Customer Satisfaction, http://ibm.co/29i1dy3

[13] IBM Champion challenger overview: http://ibm.co/2bXwlvY

[14] Bangladesh Bank exposed to hackers by cheap switches, no firewall: police, http://reut.rs/1NEgsfX

[15] IBM 2015 Cyber Security Intelligence Index for Financial Services, http://ibm.co/1OuLHsl

[16] IBM 2016 Cyber Security Intelligence Index http://ibm.co/2aeiifZ

[17] Key findings from the 2016 Cost of Data Breach Study: Global Analysis, http://ibm.co/2aKQjnV

[18] Reviewing a year of serious data breaches, major attacks and new vulnerabilities, http://ibm.co/2aeiifZ

[19] CVE and CCE Statistics Query Page, https://web.nvd.nist.gov/view/vuln/statistics

[20] Infosecurity-magazine.com, Companies Take an Average of 100-120 Days to Patch Vulnerabilities, http://bit.ly/1KUl0wX

[21] 2015 State of Vulnerability Risk Management, http://bit.ly/1U92gjP

[22] Digital Guardian website "What is Endpoint Security? Data Protection 101 http://bit.ly/28Pbipr

[23] Majority CEOs unwilling to share cybersecurity information with outsiders, Eileen Yu, http://zd.net/20E8KZb

[24] https://www.fsisac.com/about

[25] http://www.dtcc.com/news/2014/september/24/fs-isac-and-dtcc-announce-soltra.aspx

[26] Slaw, Cybercrime: Be Ready with an Incident Response Plan, http://bit.ly/29WNAaR

Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
September 2016

FDW12348-USEN-00