LOCKHEED MARTIN

Guide to Cybersecurity for Financial Services Firms

Embracing an Intelligence Driven Defense®

An eBook Presented by:
Lockheed Martin Corporation

Table of Contents

Introduction

Businesses of all sizes in every industry have grown increasingly concerned about cybersecurity, but none more so than the financial services sector. Much of a financial organization's valuable information is stored electronically, more systems and databases are in use, and use of the Internet and mobile technologies for data transmissions is growing exponentially. The risk of a cyberattack is immense.

Beyond protecting data such as customer records, clearing and trading information or confidential documents, financial services organizations have the hefty challenge of safeguarding their systems and networks as well as the financial assets they hold. While the financial, reputational, and legal ramifications of a security breach for an individual firm may be significant, if several institutions were to be attacked simultaneously, the blow to market confidence and the nation's financial stability would be disastrous.

The implications are so great that the U.S. Director of National Intelligence has ranked cybercrime as the top national security threat, saying the risk is "higher than that of terrorism, espionage, and weapons of mass destruction."[1] The systemic danger posed by cybercrimes against the financial services industry has raised concerns of regulators around the globe.

Their concerns are justified. According to the "2015 Industry Drill-Down Report" from Websense, the financial services sector encounters attacks 300 percent more frequently than other industries.[2] In just the first half of 2015 alone, the Identity Theft Resource Center tallied 30 known breaches in the financial sector.[3]

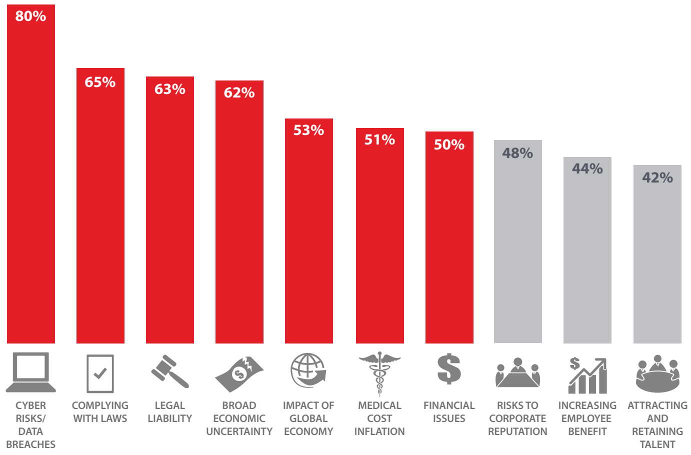
While cyber intrusions have grown more sophisticated over the last five years, banks and financial services organizations have found themselves also encumbered with challenging initiatives to improve profit margins, meet customer demands, and comply with new regulations. As they focused on these initiatives, they became more vulnerable to a variety of sophisticated and persistent cyberattacks.

Business leaders have acknowledged the wake-up call. According to the "2015 Travelers Business Risk Index," 80 percent of leaders in the banking and financial services sector cite cyber risks as their top concern, overshadowing compliance, legal, and economic concerns.[4] Many have taken steps to strengthen their cybersecurity posture, but the industry will continue to be challenged by the speed of technological change and the increasingly sophisticated nature of cyberthreats. The war against cybercrime in financial services has just begun.

In order to thwart emerging attacks, an effective defense requires a continuous effort based on an understanding of those threats and the ability to dynamically adapt to an adversary's methods. The best defense is an intelligent defense.

GREATEST RISK CONCERNS FOR THE BANKING AND FINANCIAL SERVICES INDUSTRY

How much do you worry about this threatening you business?



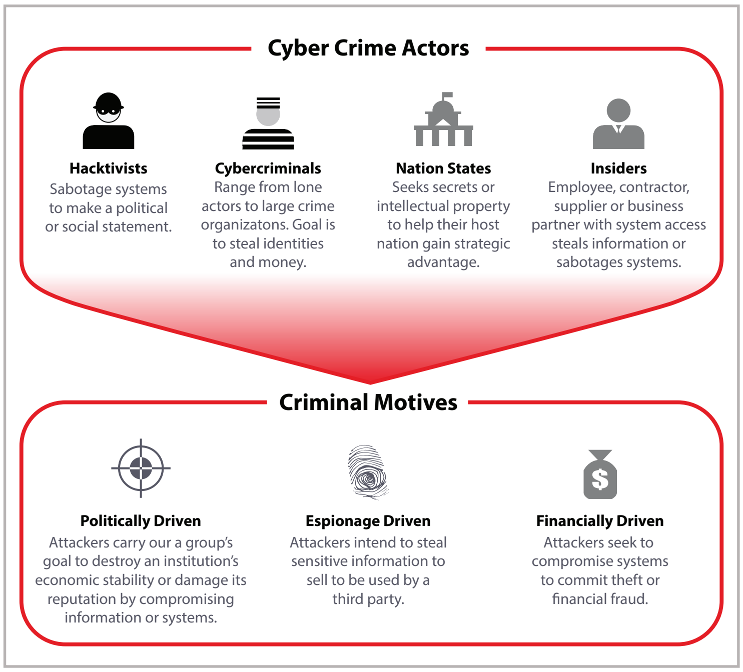
SOURCE: 2015 Travelers Business Risk Index

The goal of this guide is to help security leaders understand the risks cyberattacks present to their companies, who and what they are up against in the world of cybercrime, and why their organizations are vulnerable. It presents a cybersecurity model for organizations to detect, mitigate, and effectively adapt to advanced cyberthreats.

I. THE FACE OF TODAY'S CYBERCRIMINAL

In early 2015, a Russian cybergang was prosecuted for infiltrating more than 100 banks, financial institutions, electronic payment platforms, and financial processing firms in 30 countries.[5] Through a series of advanced persistent threat (APT) attacks, the hackers penetrated internal systems and began slowly and quietly manipulating account balances, seizing control of ATMs, and moving money out of bank accounts. Total losses are expected to reach $1 billion as the investigation continues.[6]

Money has been and will continue to be a leading motivator for criminals to target financial organizations; however, stealing customer identities, confidential documents, and even employee records can be an objective as well. The global economic crisis, increased exposure to foreign intelligence entities, and the propagation of digital data have resulted in the rise of malicious attacks from a larger pool of threat actors—hacktivist groups motivated by political or social agendas and nation-states seeking to create systemic chaos in the financial markets. Another growing threat to the financial services industry are malicious and unwitting company insiders—employees, contractors, suppliers, and even trusted business partners who have authorized access to systems and/or sensitive information.



Cyber Crime Actors

Hacktivists
Sabotage systems to make a political or social statement.

Cybercriminals
Range from lone actors to large crime organizatons. Goal is to steal identities and money.

Nation States
Seeks secrets or intellectual property to help their host nation gain strategic advantage.

Insiders
Employee, contractor, supplier or business partner with system access steals information or sabotages systems.

Criminal Motives

Politically Driven
Attackers carry our a group's goal to destroy an institution's economic stability or damage its reputation by compromising information or systems.

Espionage Driven
Attackers intend to steal sensitive information to sell to be used by a third party.

Financially Driven
Attackers seek to compromise systems to commit theft or financial fraud.

According to a security survey of the financial services sector, almost half (46 percent) of security specialists cited abuse or misuse by internal employees or contractors as their most predominant cause of breaches.[7] A disgruntled or cash-strapped insider may be easily persuaded to expose sensitive information or use it for personal gain, misuse his/her access to internal networks and systems, or create backdoor accounts to provide direct access to sensitive information.

One of the 10 largest banks in the world lost control of 27,000 customer files, potentially worth millions on the black market, to an employee who was allegedly planning to sell the stolen information.[8] At a large insurance company, an IT staffer was caught attempting to sell the identities of nearly 60,000 employees —information he had stolen from the company's database—and committed credit card fraud.[9]

Despite the number of publicized attacks, many incidents go unreported because the stakes are high. What is reported is escalating at an alarming rate. The Federal Bureau of Investigation (FBI) reports that new cases of trade-secret theft have increased 39 percent since 2010, and economic espionage cases have more than doubled in the past 18 months.[10]

Last year's hacking of a leading financial institution compromised the personal account information of 76 million households and seven million small businesses. This event accelerated efforts by federal and state authorities to push banks and brokerage firms to put more stringent procedures and safeguards in place.[11] As a result, banks and financial organizations are investing in stronger firewalls, encryption technology, and other network security measures to keep out intruders.[12]

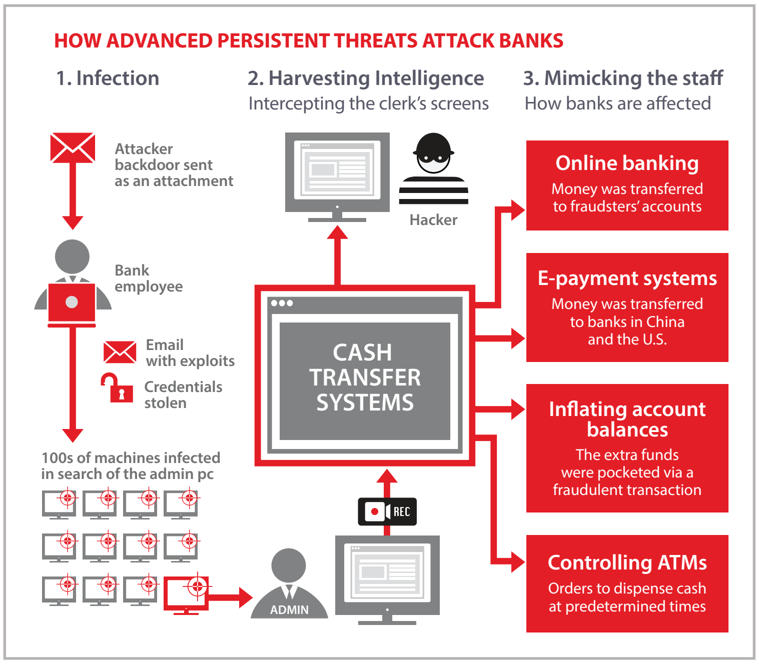
Nonetheless, given the large pool of threat actors driven by a wide range of motives, financial services firms must do more than simply strengthen their IT systems. Winning the war against cyber criminals requires organizations to embrace cybersecurity as a strategic business function, rather than an IT function, and adopt an Intelligence Driven Defense® methodology. This approach addresses the threat landscape rather than security incidents, and it continuously evolves to provide effective, predictive security based on the security status of the organization and the threats it may face. An organization that can avoid and mitigate threats no longer has to devote its security resources to reacting to incidents. That organization becomes much more secure and protected against the threats of today and those of tomorrow.

II. THE THREATS FINANCIAL SERVICES ORGANIZATIONS FEAR MOST

Safeguarding data (customer records, clearing and trading information, or confidential documents) is a priority of financial services organizations, but they must also protect their systems, networks, and the financial assets they hold. They have a greater number of "crown jewels" to steal, and so face more threats than many other industries. Following are nine of the most concerning threats:

1. **Advanced Persistent Threats (APTs)**. APTs use undetected, continuous computer hacking processes to gain access to a high-value organization's network. Phishing emails or other tricks to fool employees into downloading malware are a common practice. When the unauthorized person gains access, they often go undetected for a long period of time—quietly stealing data, committing fraud, destroying an institution's economic stability, or undermining its reputation.

   As mentioned earlier, numerous banks, financial institutions, electronic payment platforms, and financial processing firms in 30 countries (including the U.S.) were infiltrated by Russian hackers running an APT known as Carbanak. The data theft resulted in more than 160 million stolen credit card numbers, stolen identities, and hundreds of millions of dollars in losses.[13] The criminals did not need prior knowledge of the inner workings of the target banks. Instead, they used the APT to capture low-quality video of employees keying in data and used the information to withdraw an estimated $1 billion from ATMs around the world.[14]


HOW ADVANCED PERSISTENT THREATS ATTACK BANKS

1. Infection
2. Harvesting Intelligence
Intercepting the clerk's screens
3. Mimicking the staff
How banks are affected
Attacker backdoor sent as an attachment
Hacker
Bank employee
Email with exploits
Credentials stolen
100s of machines infected in search of the admin pc
CASH TRANSFER SYSTEMS
REC
ADMIN
Online banking
Money was transferred to fraudsters' accounts
E-payment systems
Money was transferred to banks in China and the U.S.
Inflating account balances
The extra funds were pocketed via a fraudulent transaction
Controlling ATMs
Orders to dispense cash at predetermined times

2. **Insider and Internal Threats**. Any employee, contractor, supplier, or business partner who has authorized access to systems and/or sensitive information has the opportunity to do irrevocable harm to a company. This threat has grown more substantial with the increased use of personal devices in the workplace, personal email, and cloud-based and USB storage devices. Intentionally or unintentionally, insiders can undermine systems, open them to malicious intrusion and engage in fraud, theft, or market manipulation.

   Case in Point: A system administrator at one of the world's largest banks developed a "logic bomb" to disable much of the bank's network. The employee had made numerous financial bets on the company's stock and meant to tank its value.[15]

3. **Denial of Service Attacks (DDoS)**. These threats are defined as "any attack intended to compromise the availability of networks and systems" and are of concern to financial corporations operating consumer-facing websites or trading systems. Such attacks flood a network with phony connection requests, making it unavailable to process legitimate user requests.

   According to a recent Verisign report, the financial services industry is experiencing an increase in DDoS attacks that camouflage other types of network intrusions. While intrusion-response teams focus on DDoS mitigation, attackers have a greater chance of getting past firewalls unnoticed to conduct data and financial theft.[16]

4. **Account Takeovers**. Cybercriminals have quickly discovered how to exploit financial and market systems that interface with the Internet, such as the automated clearing house (ACH) systems, card payments, and market trades. Exploiting system users rather than the systems themselves earns criminals access to existing bank or credit card accounts or financial systems, and allows them to carry out unauthorized transactions. According to a recent report on cybersecurity in the banking sector, almost half (46 percent) of institutions reported account takeovers as the most frequent cyber intrusion activity they experience.[17]

   One U.S. bank was held liable for $560,000 in fraudulent transfers made from one of its business account holders after their bank account credentials were compromised by a

"Last year's massive data breach of 40 million debit and credit card accounts is believed to be caused by hackers who broke into the retailer's network using login credentials stolen from a heating and cooling supplier."

targeted phishing attack.[18] The courts ruled that the bank should have been able to identify and stop the fraudulent transfers.

5. **Securities and Market Trading Breaches**.
   Financial institutions in the securities and brokerage business and their customers are frequently targeted by cybercriminals. According to the FBI, market manipulation and unauthorized stock trading are common risks faced by traders and the exchanges on which they are sold.[19] In fact, a survey of 46 global securities exchanges conducted by the International Organization of Securities Commissions and the World Federation of Exchanges Office found that more than half (53 percent) had experienced a cyberattack.[20]

6. **Third-Party-Payment Processor Breaches**.
   Sophisticated cyber criminals are also pursuing the computer networks of large payment processors, resulting in the loss of millions of dollars and the compromise of personal information of millions of individuals. One of the most costly data breaches in recent times occurred when attackers made off with close to 100 million debit and credit card numbers held by a large payroll processing company. The attack resulted in $140 million in fines and other penalties.[21]

7. **Supply Chain Infiltration**.
   Trusted suppliers of technical, computer and security equipment, software and hardware have been under attack in recent years by cyber-criminals seeking to gain physical and technical access to financial institutions. Cybercriminals are continually devising new ways to infiltrate financial institutions—from posing as vendor employees to delivering infected equipment. Some of those attacks involved hardware installed in bank branch systems to enable transactions to be manipulated via mobile networks.[22]

   Last year's massive data breach of 40 million debit and credit card accounts is believed to be caused by hackers who broke into the retailer's network using login credentials stolen from a heating and cooling supplier.[23] Once inside the network, attackers uploaded malware programs to the company's point of sale (POS) systems. The retailer's failure to properly segregate its payment processing systems within its network resulted in $10 million in settlement charges and $6.75 million in legal fees.[24]

8. **Mobile Banking Breaches.**
   Meeting customer demands for greater mobile banking capability has opened financial institutions up to another cyber threat. Cybercriminals have quickly figured out how to exploit the vulnerabilities in mobile technology by using malicious websites, text messages or mobile applications to gain access to a user's credentials and account information.

   One of the newest mobile-wallet payment systems, Apple Pay™, was hit earlier this year by a wave of fraudulent transactions using stolen credit card numbers.[25] The attack exposed a glaring weakness in mobile payments: the lack of two-factor authentication.

9. **Payment Card Skimming**.
   A skimmer fitted to the outside or inside of an ATM, POS device or gas station pumps enables a criminal to collect card numbers and personal identification numbers. The stolen data is usually sold or used to make fake cards to withdraw money from the compromised accounts. As companies continue to roll out—and consumers embrace—new electronic and wireless payment systems, criminals are quickly adapting. Hackers have already designed Bluetooth-enabled wireless skimmers to instantly download data when in range of the wireless network.

   According to a recent FICO® report, debit card fraud has hit a 20-year high.[26] Fraud at bank branch ATMs increased 174 percent over the prior year period, while off-site ATM machines rose an astounding 317 percent.[27] A 2013 heist demonstrated how quick and profitable these attacks can be: Thieves in New York withdrew $2.4 million from 2,904 machines over 10 hours—a heist prosecutors claim to be one of the largest in New York City history.[28]

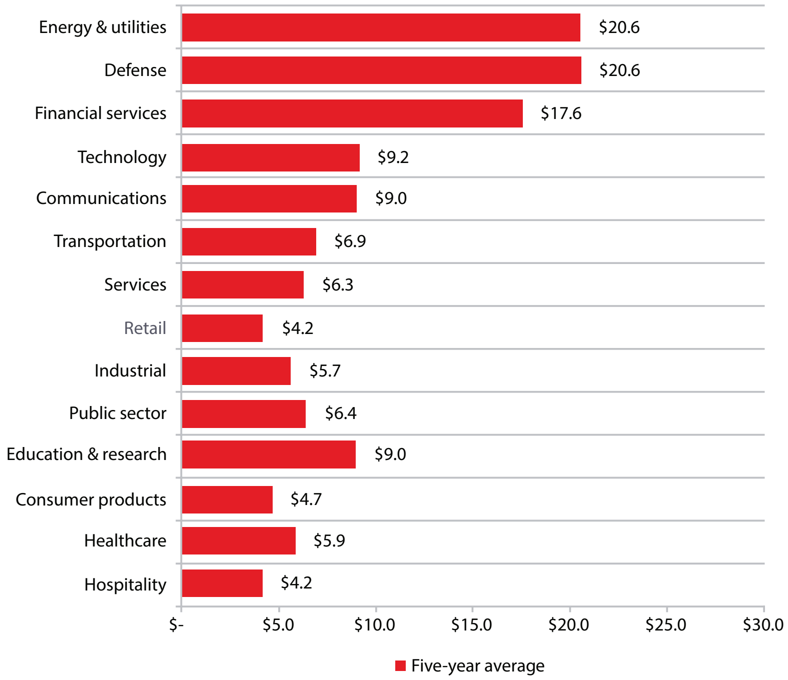
Clearly, the threats against the financial services industry are sizable and significant, but do organizations fully understand the risks they face?

III. WHAT'S AT RISK? MORE THAN THE BOTTOM LINE

> "There are simply more cyberattacks, the cost to investigate and remediate breaches has risen, and companies are losing more customers after data breaches (and subsequently revenue)."

The number of high-profile intrusions and data breaches within the financial services industry demonstrates that cyberattacks are a very real and costly concern, both domestically and abroad. According to the Ponemon Institute, the annual average cost per U.S. company of a successful cyberattack increased to $20.8 million in the financial services industry, surpassed only by the defense, energy and utilities sectors.[29]

Average Cost of a Successful Cyberattack by Industry (2010-2014)



SOURCE: 2014 PONEMAN INSTITUTE, 2014 COST OF CYBER CRIME STUDY (US)

The hefty price tag is due in part to the amount of time it takes an organization to resolve or contain cybercrimes. The Ponemon Institute found, across multiple industries, it took an average of 45 days to resolve cyberattacks with an average cost of $35,647 per day and totaling a whopping $1,593,627 over the 45-day remediation period.[30] However, before an attack can be resolved it must be identified.

The Ponemon Institute study revealed that **financial services organizations take an average of 98 days to identify an attack.**[31]

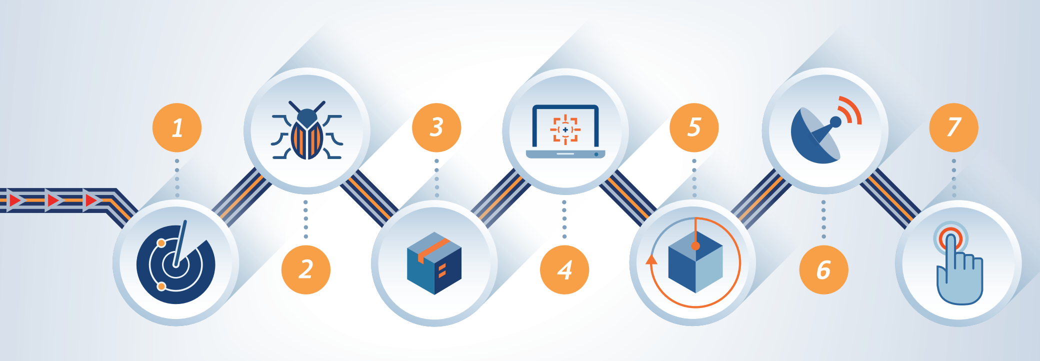
It should come as no surprise that companies are dolling out more to prevent breaches. There are simply more cyberattacks, the cost to investigate and remediate breaches has risen, and companies are losing more customers after data breaches (and subsequently revenue). In fact, according to the Ponemon Institute, between 2013 and 2014 the average loss of customers who were directly affected by a data breach increased an alarming 15 percent.[32]

Beyond the financial consequences and lost customers, organizations can be impacted by data breaches in other ways:

- Damaged brand reputation and lost investor confidence when a sensitive data breach is exposed
- Issuance of regulatory fines for insider trading or non-compliant use of customer data
- Lost clients (and subsequent lost revenue) when confidential contracts, pricing agreements or strategies are leaked
- Legal repercussions when confidentially agreements are broken
- Increased security risk when knowledge of an enterprise's business practices, systems, and databases are known
- Loss of critical and high-value personnel when salaries, perks, or employment contract details are shared
- Loss of competitive position when intellectual property is stolen
- Business disruption when critical infrastructure(s) are destroyed or compromised

Clearly, stronger efforts by the financial services industry to thwart cyberattacks are needed, but what's holding them back?

IV. WHY ORGANIZATIONS ARE AT RISK



Cyber Kill Chain® solutions Cyber Threat Model © 2011 Lockheed Martin Corporation. All rights reserved

> "The Lockheed Martin Cyber Kill Chain® is a valuable tool for security professionals to continuously collect and understand intrusions, and dynamically adapt to an adversary's methods."

Cyberattacks against the financial community are happening more rapidly than ever before, yet organizations are lagging to react and put more sophisticated, comprehensive safeguards in place. The following paragraphs discuss some of the reasons why this is happening:

Focused Solely on Financial Crime

While safeguarding systems against financial theft will continue to be a necessity, financial services organizations must address the fact that they are not dealing with financial crime only. As outlined earlier, they face a far greater number of threats than any other industry—threats driven by well-organized actors who are interested in more than stealing money. Hacktivist groups fueled by social or political agendas intent on compromising information or systems, and nation states seeking to steal intellectual property or trade secrets, are very real threats to the industry.

What Should Happen Next? Organizations need to adopt a broader view of who (actors) they are being targeted by, what (data, systems, etc.) is at stake, and how (threats) they are being targeted. The Lockheed Martin Cyber Kill Chain® is a valuable tool for security professionals to continuously collect and understand intrusions, and dynamically adapt to an adversary's methods. With this broader view, organizations can more easily establish cybersecurity baselines, identify gaps, develop strategic road maps and strengthen their cybersecurity positions.

Misguided by Compliance

Following the global financial crisis, many in the industry invested heavily in technology to meet a laundry list of regulatory requirements. Since then, regulatory (and industry) compliance has been closely linked with information security, and often has been the lever (or hammer) by which organizations made necessary investments in security. But being compliant and being secure are very different. In too many cases, banks and other financial institutions that were deemed compliant were also breached.

One issue with present-day cybersecurity risk management practices driven by compliance requirements is they are often managed as IT functions. This approach focuses on security controls and vulnerabilities, creating highly reactive (rather than proactive) operational environments. When vulnerabilities and incidents are found, they are handled at a micro level rather than using intelligence to develop larger-scale threat scenarios and patterns.

What Should Happen Next? Companies must ensure that regulatory compliance does not come at the price of protecting against targeted attacks. Defensive efforts focused on out-of-the-box IT solutions are not enough to prevent a large-scale attack. Financial service organizations need to embrace cybersecurity as a strategic business function and employ cutting-edge technology, vigilant people, and innovative methods to achieve an efficient, effective response to active threats and potential incidents.

Misunderstanding Business Resilience

Among many CIOs, business resilience is thought of as continuity or disaster recovery. However, in today's digital world the term "availability" does not just apply to IT systems, but to the people, processes, and technology that drive business value. In short, business resiliency is an organization's ability to recognize threats before they happen, reduce the organization's exposure to harm and, most importantly, react quickly.

Organizations are shifting, albeit slowly, as more board members and risk executives are being held accountable for business resilience—either through regulatory efforts or litigation after a breach.

What Should Happen Next? Boards that fund cybersecurity technology looking for a silver bullet to risk management will be disappointed. Today they must adopt a broader view—that building an enterprise's cybersecurity strength is about building a resilient business rather than simply reducing financial risk. Forward-thinking boards will fund cybersecurity initiatives with resources and solutions that take a more holistic approach. This approach goes far beyond a return on investment (ROI) model; it considers the cost of lost reputation and market share versus overhead, fines and lost revenue resulting from a breach.

Exposed by New Technologies

Compounding the security challenges faced by the financial services sector is the need to attract new customers and retain existing ones. The "consumerization" of technology has put increasingly powerful devices into the hands of customers who expect anywhere, anytime access to information and services. This has created new channels for banking, lending, investment management, and insurance with the potential to attract new customers, but with it come new challenges for security teams. Cybercriminals, seeing more transactions taking place on mobile devices and over the Internet, are adjusting their approaches to infiltrate and gain access through these channels.

The threat of data theft is further heightened by the bring-your-own-device (BYOD) to work movement. Most companies, driven by a desire to improve employee productivity and satisfaction, are openly embracing the trend. Few, however, are addressing the potential risks. One survey found that only 11 percent of enterprises explicitly restrict employee use of personal devices to access enterprise data.[33]

Social media is also emerging as an important customer channel. Nearly 75 percent of banking employees are making use of social media, yet only 20 percent of banks have deployed technical controls to block or limit organizational usage.[34] This opens up a new window of opportunity for criminals to use social engineering to target victims or spread infected links.

What Should Happen Next? The challenge for the financial services industry is to find a balance between protecting an organization's information and assets and the needs of its employees, partners, and customers for on-demand access to information. Establishing usage policies that manage risk, but won't hinder productivity, and a formal program to educate employees on proper use of new technologies and their related risks to the organization is critical.

Encumbered by Silos

Information silos represent a major IT security challenge for financial services firms. Information silos—IT systems that are accessible by, but do not fully interoperate with, other systems—can be created intentionally to protect critical or sensitive information. More often, however, silos develop over time through the acquisition of incompatible systems.

The financial services industry can be particularly vulnerable to this problem due to rapid consolidation of organizations through mergers and acquisitions. The IT systems, proprietary technology, policies, and security operations of acquired companies are often connected without being fully integrated. As long as the legacy systems continue to function and perform their tasks, the expensive and time-consuming job of replacing or re-engineering them often is delayed. The result is a patched-together network of incompatible code, tools, technology, processes and organizations that are difficult to manage and monitor.

Silos also limit visibility across the IT enterprise, reducing productivity and creating risk by providing opportunities for intruders to hide while exploring systems in search of accounts, sensitive information, and intellectual property. In a fragmented infrastructure, an intruder who gains access to one system—even if it is not mission-critical—can use it as a base to safely move to more sensitive and critical areas that can be exploited.

What Should Happen Next? Organizations need to develop comprehensive security models that address legacy systems as well as new resources such as cloud services, mobile devices, and applications. Furthermore, integrating information silos more fully into the enterprise can help to better detect and isolate breaches and other security incidents, improve situational awareness, and reduce enterprise risk.

Despite the challenges of meeting regulatory demands, ensuring business resilience, adopting new technologies, and working with siloes and legacy systems, financial services organizations can evolve their security operations to achieve the highest levels of cybersecurity protection.

V. HOW ORGANIZATIONS CAN PROTECT THEMSELVES

Security is no longer a one-size-fits-all solution. Instead, companies must take a holistic approach to creating programs that work. Technologies evolve and create new threats and vulnerabilities for organizations to address. As such, security organizations need to evolve in order to combat emerging cyber adversaries.

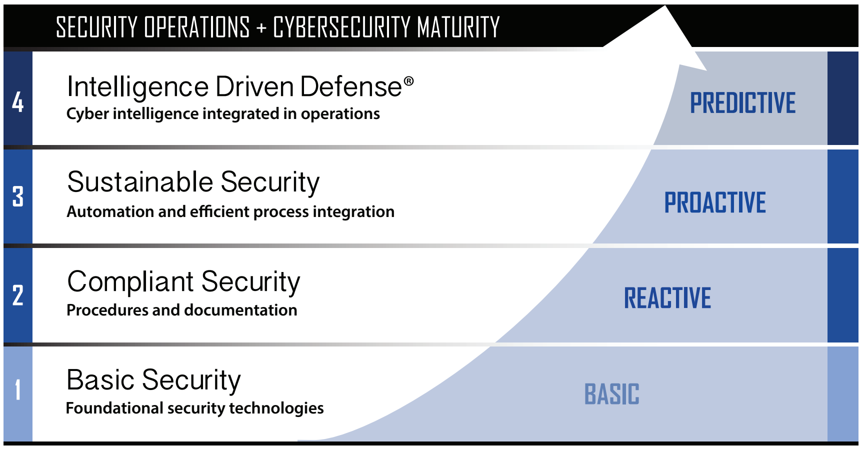
Present-day cybersecurity risk management practices within the financial services industry are primarily driven by compliance requirements and managed as an IT function. This approach, unfortunately, focuses on security controls and vulnerabilities, creating highly reactive (rather than proactive) operational environments. When vulnerabilities and incidents are found they are handled at a micro level rather than using the intelligence to develop larger-scale threat scenarios and patterns.

Today's threat landscape requires organizations to take a proactive approach to security, rather than merely reacting to threats, helping to address them before they cause harm. This level of cybersecurity maturity supports an Intelligence Driven Defense® posture—the leveraging of intelligence to become proactive and predictive rather than maintaining a "firefighter" approach.

The organizational goal should be to mature the security posture to one of a defense driven by intelligence. Achieving that goal requires a thorough examination of tools, processes, and procedures currently in place to determine if they are properly defending against sophisticated threats and protecting the enterprise. This is a journey Lockheed Martin embarked on over a decade ago with its own cybersecurity operations to adapt to the evolving landscape—we developed Intelligence Driven Defense® branded cyber technologies, skill sets, and tradecraft to fortify our computer systems across our enterprises.

Four levels of cybersecurity maturity are found in today's organizations.

1. **Basic Security Operations** have a foundation of network hardware, software and limited fault monitoring systems including IPS, IDS, firewalls, and SIEM systems. These tools keep a firm insulated from 80 percent of known threats. However, they largely fail against advanced persistent threats and do little to identify dangerous insiders.
2. **Compliant Security Operations** build on basic security by introducing specific procedures and documentation practiced by a network operation center or a security operation center (SOC). The focus is to deploy more rapid mitigation of cyber intrusions and create a reactive defense posture. Often significant gaps exist in placed controls.
3. **Sustainable Security Operations** align the procedures and documentation with industry best practices or regulatory compliance standards for the domain. These are dedicated facilities that defend the entire enterprise and respond to all forms of security threats. These traditional centers serve well in response to traditional attacks, but today's threat landscape requires organizations to take a predictive approach to security so threats may be addressed before they cause harm, versus merely reacting to them.
4. **Intelligence Driven Defense®** services can help evolve a traditional SOC into a security intelligence center (SIC). People and technology are still crucial elements, however both are evolved and tailored to support a mature posture. Intelligence Driven Defense® is driven by organizational collaboration, intelligence and event analysis, and early threat detection. Threat intelligence is consumed, produced and used to strengthen the financial institution's security posture with a predictive capability that puts the organization in a position to respond to evolving threats before they occur.


SECURITY OPERATIONS + CYBERSECURITY MATURITY
4
Intelligence Driven Defense®
Cyber intelligence integrated in operations
PREDICTIVE
3
Sustainable Security
Automation and efficient process integration
PROACTIVE
2
Compliant Security
Procedures and documentation
REACTIVE
1
Basic Security
Foundational security technologies
BASIC

When assessing a firm's cybersecurity maturity, Lockheed Martin examines 15 key process areas of an organization's operations and rates them on a four point scale. Download our sample **4.0 Cybersecurity Maturity Self-Assessment Scorecard** for an outline of key considerations for each process area and description of an ideal 4.0 state.

Enlisting the Help of Security Experts

Mixing new digital banking practices with traditional cybersecurity can quickly overwhelm security teams relying on a reactive approach. Getting the right advice can help firms realize the benefits of new cybersecurity models while eliminating or mitigating new risks. As such, many organizations are enlisting the help of security organizations like Lockheed Martin to understand today's sophisticated threats and bring expertise and industry best practices to their security operations.

Lockheed Martin leverages decades of cybersecurity—to deliver intelligence-driven solutions and services that assist organizations as they evolve to fight the threats of today and build to scale for the threats of tomorrow. Here is a five-step approach that uses Lockheed Martin services and tools to help organizations evolve their security practices and stay ahead of adversaries.

Assess Your Threat Profile

Understanding how your institution's activities, connections and operational procedures might put the company at risk is an important first step. Our **Assessment Services** help organizations assess their cybersecurity maturity level and understand their level of preparedness to take on adversaries. For example, in the event of 100 different attacks, how many would be successful and how many would be identified and blocked? We work with your security teams to identify threats to information or information systems, determine the likelihood of a threat occurrence, and identify where system vulnerabilities exist.

Develop a Protection Strategy

When threats, vulnerabilities, and risks have been identified, the next step is to ensure appropriate safeguards are in place to mitigate an attack or breach. Using Intelligence Driven Defense® solutions result in a more cost-effective and efficient overall security response based on an understanding of the organization's security profile, the threat landscape in which it operates, and improved situational awareness. Our **Professional Services** team assists in establishing and implementing a strategic vision that incorporates the requirements for an effective enterprise security posture. We use our proprietary **Cyber Kill Chain**® to analyze intrusions, extract indicators, and create a tailored strategy and implementation plan that will achieve the most sensitive defensive goals. This includes developing a concept of operations plan; allocating required resources including people, training, and security tools; and establishing locations for security operations.

Train Your Employees

Strengthen your employee training program with our comprehensive user-awareness program, **The I Campaign**®. This program helps organizations improve their security culture by establishing a baseline of existing risky behavior through the use of simulated phishing testing and training, educating employees on individual responsibility, and measuring improvements.

Lockheed Martin Helps Global Firm Improve Cybersecurity Operations

Despite multiple computer emergency readiness teams and security operations centers across its organization, a multinational banking and financial services corporation had little insight into internal and external threats. The company turned to Lockheed Martin to develop a strategic vision for its security operations and coordinate its disparate security systems.

Solution

By utilizing Lockheed Martin's **Cyber Kill Chain**®, the organization's security team was able to identify and assess threats in a uniform way. This was a critical first step in developing the appropriate strategy and supporting road map, including the design and creation of a fusion center—an umbrella program to coordinate all the organization's security systems. Lockheed Martin further assisted the company with integrating its network and implementing best-practice processes and workflows.

Results

The introduction of a proactive, centralized center of intelligence for all its enterprise assets and data flows improved the company's hit rate on real cyber threats by 20 percent in just six months. Additionally, the company was able to reduce its global security staff by 15 percent, resulting in significant cost savings.

Identify Technology Reinforcements

The baseline of any detection strategy includes monitoring systems, such as IPS, IDS, firewalls, and SIEM systems. It often requires more sophisticated tools to incorporate **Intelligence Driven Defense**® solutions into an existing operations center. Recommendations may include our **Palisade**® centralized platform, which integrates into existing security infrastructures to deliver enterprise-wide visibility, awareness and alerting capability. To zero in on individuals of greatest concern inside the organization, the **LM Wisdom® Insider Threat Intelligence** (ITI) solution evaluates employee attributes, behaviors, and actions based on data merged from disparate enterprise systems including performance reviews, human resource information, and counterintelligence from analyst-defined models.

Support Your Ongoing Efforts

To further assist organizations with their cybersecurity efforts, we offer several management service solutions. Our **Advanced Threat Monitoring Service** integrates APT sensors into your existing environments to give our cybersecurity analysts a wider view of IT assets and critical network infrastructure. If we detect anomalies,

> “Lockheed Martin leverages decades of cybersecurity expertise—defending the most attacked network in the world—to deliver intelligence-driven solutions and services that assist organizations as they evolve to fight the threats of today and build to scale for the threats of tomorrow.”

we work with your security team to quickly mitigate the risk. And finally, we can provide added intellectual property security by directing domain name system (DNS) requests to secure Lockheed Martin DNS servers through our **Domain Name System Blocking** solution.

Working with Lockheed Martin

Cyber technology will continue to evolve to give financial services organizations more opportunities to grow their businesses and improve their operations. But cyberthreats will continue to grow as well. Given the sizable financial, reputational, legal, and market ramifications cyber intrusions can inflict, the industry can no longer afford to defend itself with limited, reactive security approaches. The next evolution in cybersecurity is to develop a defense driven by intelligence that employs cutting-edge technology, vigilant people, and innovative processes.

For over a decade, Lockheed Martin has been a trusted partner to financial services organizations around the globe, helping them protect their enterprise assets, intellectual property and employees. Lockheed Martin’s holistic approach to cybersecurity offers comprehensive security services and technologies that ensure an adaptive defense strategy and mature security posture—the top choice for the financial services industry.

Learn more about Lockheed Martin’s services and technology at **http://cyber.lockheedmartin.com**.

VI. ENDNOTES

[1] "Threats to the Financial Services Sector," 2014, PwC, Retrieved from https://www.pwc.com/en_GX/gx/financial-services/publications/assets/ pwc-gecs-2014-threats-to-the-financial-services-sector.pdf.

[2] Adam Greenberg, "Report: Security Incidents in Finance Sector 300 Percent More Frequent Than Other Industries," 24 June 2015, SC Magazine,Retrieved from http://www.scmagazine.com/financial-services-firms-see-three-times-more-security-incidents-than-other-sectors/article/422655/.

[3] ITRC Breach Reports, 8 September 2015, Identity Theft Resource Center, Retrieved from http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.

[4] "Travelers 2015 Business Risk Index Summary," May 2015, Travelers Insurance. Retrieved from https://www.travelers.com/prepare-prevent/risk-index/business/2015/business-risk-index-report.pdf.

[5] Jo Ling Kent, "How Cyber Criminals Stole up to $1B from Financial Services Companies," 16 February 2015, FOX Business, Retrieved from http://www.foxbusiness.com/2015/02/16/how-cyber-criminals-stole-up-to-1b-from-financial-services-companies/.

[6] Jo Ling Kent, "How Cyber Criminals Stole up to $1B from Financial Services Companies," 16 February 2015, FOX Business, Retrieved from http://www.foxbusiness.com/2015/02/16/how-cyber-criminals-stole-up-to-1b-from-financial-services-companies/s/.

[7] Security Spending and Preparedness in the Financial Sector: A SANS Survey, 2015, SANS Institute, Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/security-spending-preparedness-financial-sector-survey-36032.

[8] Chris Preimesberger, "The Seven Largest Insider-Caused Data Breaches of 2014," 29 December 2014, eWeek.com, Retrieved from http://www.eweek.com/security/slideshows/the-seven-largest-insider-caused-data-breaches-of-2014.html.

[9] Larry Greenemeier, "How To Spot Insider-Attack Risks In The IT Department," 8 December 2006, Retrieved from http://www.informationweek.com/how-to-spot-insider-attack-risks-in-the-it-department/d/d-id/1049722?

[10] "2013 Joint Strategic Plan on Intellectual Property Enforcement," June 2014, U.S. Intellectual Property Enforcement Coordinator, Retrieved from http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

[11] Jessica Silver-Greenberg & Matthew Goldstein, "After JPMorgan Chase Breach, Push to Close Wall St. Security Gaps," 21 October 2014, New York Times, Retrieved from http://dealbook.nytimes.com/2014/10/21/after-jpmorgan-cyberattack-a-push-to-fortify-wall-street-banks/?_r=0.

[12] Sharone Tobias, "2014: The Year in Cyberattacks," 31 December 2014, Newsweek, Retrieved from http://www.newsweek.com/2014-year-cyber-attacks-295876.

[13] "Russian National Charged in Largest Known Data Breach Prosecution Extradited to United States," 17 February 2015, United States Department of Justice, Retrieved from http://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states.

[14] GReAT, "The Great Bank Robbery: the Carbanak APT," SecureList, 16 February 2015, Retrieved from https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/.

[15] Larry Greenemeier, "How To Spot Insider-Attack Risks In The IT Department," 8 December 2006, Retrieved from http://www.informationweek.com/how-to-spot-insider-attack-risks-in-the-it-department/d/d-id/1049722?

[16] Roy Urrico, "Financial Services Industry Attacks Increase," Credit Union Times, 3 June 2015, Retrieved from http://www.cutimes.com/2015/06/03/financial-services-industry-attacks-increase.

[17] "Report on Cybersecurity in the Banking Sector," May 2014, New York State Department of Financial Services, Retrieved from http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf.

[18] "Failure to Conduct Proper Email Notifications on Account Usage and Changes Costs One Bank Over $400,000, 31 July 2012, The Fraud Practice, Retrieved from http://www.fraudpractice.com/News-BankClientACHFraudBattles.html.

[19] Gordon M. Snow, "Cybersecurity: Threats to the Financial Sector," 14 September 2011, Federal Bureau of Investigation, Retrieved from https://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector.

[20] "Cyber-crime, Securities Markets and Systemic Risk," July 2013 , IOSCO and the World Federation of Exchanges Office, Retrieved from http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf.

[21] Dave Lewis, "Heartland Payment Systems Suffers Data Breach," 31 May 2015, Forbes, Retrieved from http://www.forbes.com/sites/davelewis/2015/05/31/heartland-payment-systems-suffers-data-breach/.

[22] "Threats to the Financial Services Sector," 2014, PwC, Retrieved from https://www.pwc.com/en_GX/gx/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf.

[22] Ivy Schmerken, "Morgan Stanley Data Theft Exposes Insider Threat & Need for More Restrictions," 14 January 2015, Information Week, Retrieved from http://www.wallstreetandtech.com/security/morgan-stanley-data-theft-exposes-insider-threat-and-need-for-more-restrictions/d/d-id/1318623.

[23] Jaikumar Vijayan, "Target Breach Happened Because of a Basic Network Segmentation Error ," 6 February 2014, Computer World, Retrieved from http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html.

[24] Hadley Malcolm & Elizabeth Weise, "Few Target Victims to Benefit From Settlement," 20 March 2015, USA TODAY, Retrieved from http://www.usatoday.com/story/money/2015/03/19/target-breach-settlement-details/25012949/.

[25] Robin Sidel & Daisuke Wakabayashi, "Apple Pay Stung by Low-Tech Fraudsters," 5 March 2015, The Wall Street Journal, Retrieved from http://www.wsj.com/articles/apple-pay-stung-bylow-techfraudsters-1425603036.

[26] Robin Sidel, "Theft of Debit-Card Data From ATMs Soars," 19 may 2015, The Wall Street Journal, Retrieved from http://www.wsj.com/articles/theft-of-debit-card-data-from-atms-soars-1432078912.

[27] Robin Sidel, "Theft of Debit-Card Data From ATMs Soars," 19 may 2015, The Wall Street Journal, Retrieved from http://www.wsj.com/articles/theft-of-debit-card-data-from-atms-soars-1432078912.

[28] Marc Santoramay, "In Hours, Thieves Took $45 Million in A.T.M. Scheme," 9 May 2013, The New York Times, Retrieved from http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html.

[29] "Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis," 5 May 2014, The Ponemon Institute, Retrieved from https://securityintelligence.com/cost-of-a-data-breach-2015/.

[30] "Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis," 5 May 2014, The Ponemon Institute, Retrieved from https://securityintelligence.com/cost-of-a-data-breach-2015/.

[31] "New Ponemon Institute Survey Reveals Time to Identify Advanced Threats is 98 Days for Financial Services Firms, 197 Days for Retail," 19 May 2015, Ponemon Institute, Retrieved from https://securityintelligence.com/cost-of-a-data-breach-2015/.

[32] "Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis," 5 May 2014, The Ponemon Institute, Retrieved from https://securityintelligence.com/cost-of-a-data-breach-2015/.

[33] Yishay Yovel, "State of BYOD and Mobile Security Report: Latest Insights, Trends and Stats," 16 July 2014, IBM, Retrieved from http://securityintelligence.com/state-of-byod-and-mobile-security-report-latest-insights-trends-and-stats/.

[34] "2012 DTTL Global Financial Services Industry Security Study," 2012, Deloitte, Retrieved from http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/dttl-fsi-SecurityStudy2012.pdf.

Guide to Cybersecurity for Financial Services Firms

Embracing an Intelligence Driven Defense®

For more information on cybersecurity solutions.

Email: cyber.security@lmco.com

Phone: 855-LMCYBER

http://cyber.lockheedmartin.com

PIRA# CMK201510005 Version 1.0