Making your Enterprise Cyber Resilient

High performance. Delivered.
Financial services firms cannot protect themselves from cyber attacks 100 percent of the time. In spite of their best efforts, breaches will occur over time. That means that, in addition to increasing the sophistication of their barriers, financial institutions also need to increase their resilience—their ability to bounce back from an attack or other security event and resume normal operations.
The growing risks and costs of cyber attacks

Although the rise of digital has revolutionized how businesses work and serve their customers, it has also added new and more severe dimensions of risk for financial services firms.

Coping with these digital risks is now an urgent matter. Cyber attacks are dramatically increasing. The number of data breaches rose 23 percent in 2014. Five out of every six large companies (those with more than 2,500 employees) were attacked in 2014, a 40 percent increase over the previous year. Small- and medium-sized businesses also saw an increase, with attacks rising 26 percent and 30 percent respectively. More than 317 million new pieces of malware were created in 2014, meaning nearly one million new threats were released into the digital world each day.

The costs of cyber attacks are also soaring—measured in loss of revenue, loss of customer trust and loyalty, and costs of litigation and higher insurance premiums. According to a global insurer, cyber attacks cost businesses as much as $400 billion a year, including the initial damage as well as ongoing disruption. By 2020, research firm Gartner expects companies across the globe will spend about $170 billion on cyber security, a growth rate of almost 10 percent over the next five years. The frequency and intensity of digital risks, as well as their costs, is now affecting agency oversight. Standard & Poor’s Financial Services LLC, a part of McGraw Hill Financial (S&P), has announced that it will be considering firm’s cyber security capabilities in their credit ratings and may downgrade firms where cyber weakness has been identified. We expect others to follow.

In the face of this threat and its associated developments, financial services firms should now think differently about digital risk management. The protective steps they are taking are important but not enough. Cyber attacks are not an “if” but a “when and how.” The threats are too frequent and too varied. Attackers are nimble and adapt quickly. They require little capital investment and resources to devise and mount their attacks. Many criminals are already inside a company and breaches are inevitable in our view. Traditional preventative measures can slow them down but not ultimately stop them.

That means that firms should think differently. In addition to improving their traditional preventive measures, they also should make themselves cyber resilient.
What is cyber resiliency?

Cyber resiliency is the ability to operate the business processes in normal and adverse scenarios without adverse outcomes. Specifically, resiliency strengthens the firm’s ability to identify, prevent, detect and respond to process or technology failures and recover, while reducing customer harm, reputational damage and financial loss.

Resilient businesses have several common characteristics:

- More secure processes and systems
- Strong controls with a strong control environment
- A solid risk culture
- Digitized and automated processes

To become more cyber resilient, firms need to not only incorporate the front-end security, but also the business risk/reward decision making, risk management and control techniques, as well as secure employee adoption. Only then can they expect to more effectively mitigate the likelihood of an event and reduce the impact if one does occur.

Creating cyber resiliency should span business processes and infrastructure. For example, it should include re-architecting business processes to reduce the access, dissemination, and reliance on highly sensitive data. It should also involve re-architecting infrastructure and systems to limit the extent of potential damage when an attack occurs or systems and processes fail. And it may include re-working ways in which legal and liability protections are incorporated into service agreements to prevent fraud-related losses or expenses associated with remediating impacted customers.
Making your Enterprise Cyber Resilient

Three pillars of cyber resilience

Some firms may limit cyber resilience and risk management to just an exercise of “being prepared” for a worst-case scenario. Being prepared is certainly an important part of resilience because having a plan can help shape a proper response in a stressed scenario. However cyber risks are multi-dimensional, and cyber resilience should focus on managing three types of risks in particular. (See Figure 1.)

Figure 1. Summary of cyber risks, consequences and responses

<table>
<thead>
<tr>
<th>IT Systems and Infrastructure Risks</th>
<th>Operational Risks</th>
<th>Fraud and Financial Crime</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What are the risks?</strong></td>
<td><strong>Brand and reputational risks associated with loss of trust</strong></td>
<td><strong>Internal fraud from employees and third parties</strong></td>
</tr>
<tr>
<td>• Expansion of digital capabilities increase exposure points for penetration</td>
<td>• Failure to operate in a stable or stressed environment leading to financial losses</td>
<td>• External fraud from criminal activities</td>
</tr>
<tr>
<td>• Data loss, including Personally Identifiable Information (PII), Intellectual Property (IP), and Material Non-Public Information (MNPI)</td>
<td>• Loss of intangible value and goodwill</td>
<td>• Money laundering</td>
</tr>
<tr>
<td>• System failure, loss of system control or complete system takeover</td>
<td>• Legal and regulatory risks due to non-compliance</td>
<td>• Account take-over</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>What are the consequences?</strong></th>
<th><strong>What are the responses?</strong></th>
<th><strong>What are the responses?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Time intensive/high cost to repair</td>
<td></td>
<td>• Embrace digital processes and controls for agility and prevention</td>
</tr>
<tr>
<td>• Increased vulnerabilities/exposure</td>
<td>• Re-architect how systems and processes are designed and implemented</td>
<td></td>
</tr>
<tr>
<td>• Loss of trust/reputational risk</td>
<td>• Increase scope of accountability beyond technology and into the business</td>
<td>• Regular planning and oversight from a firm-wide perspective with business and technology accountability</td>
</tr>
<tr>
<td>• No longer able to control data once extracted from source</td>
<td></td>
<td>• Improve the effectiveness of current process and system controls</td>
</tr>
</tbody>
</table>

Source: Accenture, November 2015
IT systems and infrastructure risks

Technology systems and infrastructure are often “ground zero” for cyber attacks and other breaches, so technology risk management is increasingly important to a cyber-resilient firm. At a minimum, leading technology risk management programs incorporate the following:

- Application development standards: How applications, systems and infrastructure are architected and developed to reduce risk. Techniques may include firewalls, access management, encryption and transmission techniques.
- Systems and data surveillance: Monitoring and surveillance techniques for identifying, assessing and responding to potential vulnerabilities or breaches.
- Penetration testing: Establishing the resilience of the infrastructure to attacks and proactively identifying where vulnerabilities may occur.

Technology risk management programs should not exist in a silo or as an independent function. Instead they should be integrated with other risk management programs such as operational risk and compliance.

Technology risk management also needs greater visibility in the appropriate business governance and management routines. This is important both for funding and investment in mitigating the cyber risk, as well as advising and directing the business as future decisions are made.

Operational risks

Operational risks refer to the potential for a firm’s business processes or technology infrastructure to fail, with adverse consequences such as being unable to communicate with customers, generate transactions or conduct billing. Operational risks also impact brand and reputation, leading to the potential for losses in intangible value as well as actual sales and revenue.

An operational risk management program should incorporate the following elements as part of building cyber resiliency:

- Risk appetite: Levels that define and incorporate the tolerance and parameters by which resiliency will be established for cyber risk management programs and how cyber events will be handled.
- Process and technology risk assessments: Processes that examine gaps in controls around business processes, products or services.
- Control reviews: Effectiveness assessments that show evidence of proper controls that can prevent or detect cyber risk-related losses.
- Integrated framework: A cyber risk framework for identifying, preventing, detecting and responding to cyber risks.

A resilient organization recognizes that cyber attacks and cyber risks evolve rapidly, occur with high frequency and are unrelenting—meaning they cannot easily be isolated and managed. Therefore, the risk management models should be nimble, flexible and proactive with regard to how governance, policy, technology and processes are implemented.

Most important, the operational risk capability should be at the forefront of quantifying the risk exposure. That means working horizontally between Chief Risk Officer (CRO), Chief Information Officer (CIO) and Chief Operations Officer (COO) to encourage proper investment, maintenance and control across multiple points of entry and attack.

Fraud and financial crime

Fraud and financial crime can result from the exploitation of vulnerabilities in payment systems, digital banking services, electronic trading and failed controls in business processes, technology and even third-party organizations. Furthermore, cyber criminals often rely on the financial institution’s infrastructure to perpetrate and carry out their schemes, masking themselves as legitimate customers.

Fraud and financial crime losses can come either from large, one-time events or frequent, small and harder-to-detect, low-cost events. The fraud costs associated with a firm’s customers also impact them because they bear the brunt of losses associated with attacks using stolen identities, credit cards and account remediation—costly services for events not within their direct control.

A resilient organization should incorporate the following elements in its fraud and financial crime risk management programs:

- Surveillance: The ability to monitor and detect anomalies inside the institution is an important aspect of identifying and controlling losses tied to cyber risk.
- Detective business processes: Business processes that are designed to be both compliant and detective of criminal or nefarious activities in a proactive management technique.
- Industry data sharing: Even with new regulations on the horizon that allow data sharing of events with the federal government, industry sharing of attack data to improve detection and response techniques can help reduce unexpected losses tied to fraud and financial crime.
Why are organizations challenged in developing cyber resiliency?

Most firms are currently working on a better way to address cyber risk, but few have mastered it. Why? In our view, companies face at least four types of challenges:

1. **Organizational silos**
Cyber risk is often viewed as a technology limitation managed by security (physical or cyber), and is typically owned by the Chief Information Security Officer (CISO). Disparities in risk ownership may lead to insufficient interaction with the CRO or with the business, thus limiting the visibility to frequency or impact.

2. **Insufficient business involvement**
Information security should be viewed as a business issue, not only a technology one. Companies should manage cyber security risk from a business-centric, enterprise-holistic perspective.

3. **Over-reliance on training and communications**
The weakest link in cyber resiliency is the human element. However, most cyber risk mitigation programs rely too heavily on changing human behavior as the control mechanism for cyber risk. Cyber attacks often go after the path of least resistance; however, a cyber resilient organization is able to contain that attack and not rely solely on people as the way to mitigate or control the risk.

4. **Talent shortfalls**
Similar to the silos created between CIO, CRO, COO, and CISO, talent often follows either the business or technology path, which leads to competing priorities. With high demands for technology-savvy resources, the availability of talent to build a resilient business may be limited.
A methodology for building cyber resiliency

We believe that holistic capabilities across risk and security underpin the approach to defining and delivering cyber resiliency. Financial services companies need to bring together capabilities to execute risk assessments, support effective surveillance, enhance incident response and strengthen controls to become more cyber resilient.

Our recommended methodology encompasses the full breadth of entry points and angles by which financial organizations need to build readiness and cyber resilience. (See Figure 2.)

Figure 2. A methodology for building cyber resiliency

**Respond**
- Event response plan: Structure to identify and manage action plans
- Crisis management: Structure to manage incidents and notify impacted parties

**Detect**
- Operational monitoring: Aligning the tools to identify and detect threats along with their escalation and oversight
- Detection and identification: Tools and metrics to identify and log aspects that help manage operations

**Identify**
- Risk identification: Aggregated set of typical risks associated with cyber risk
- Risk events: Scenarios that could impact the organization and are specific to cyber threats

**Prevent**
- Operating model: Specifying the structure with people, organization, roles, tools and processes to govern
- Business and IT controls: Oversight of controls and their testing programs

Source: “How to Make Your Enterprise Cyber Resilient,” Accenture, October 2015
Identification:  
What is the impact?

Organizations should develop the capability to quickly identify where a cyber attack is taking place so that they can prevent, detect and respond as necessary. What scenarios can help to proactively prevent events from happening? What are the risk mitigation strategies that a firm could put into place to address impacts before they become real?

So-called “penetration testing” has become one way to proactively identify weaknesses in a firm’s cyber defense structures. We believe firms need to go beyond executing prepared scripts and move to advanced adversary impersonation. Inside and/or outside groups are hired or assigned to attempt to breach the company’s defenses, probing networks, applications and other computer systems. Security professionals then use that information to improve their defenses.

The findings often demonstrate that the gaps and deficiencies are with the people, rather than with the technologies. Externals are able to gain access to critical information and secure areas without having to break through firewalls and other technology-based protection layers.

Better information sharing is also important. Organizations should share and have access to all threat indicators to help decrease the rate of attacks. Advanced employee training is also essential, helping them to more readily detect and be aware of cyber attacks such as phishing. With one recent high-profile hacking in the financial services industry, indications are that the hackers gained access to the firm’s data by stealing the network credentials of employees with high-level IT access.

In general, efforts should be focused on preventing and mitigating attacks and breaches instead of minimizing the cost of breaches after they occur.

Prevention:  
How do we organize?

The questions at the heart of prevention include such things as: How do we control our environment? How do we establish the proper technology hygiene in terms of developing and coding systems? How do we see that proper access is in place—using things like ISO standards for how systems are developed or how they’re accessed or reviewed, and also how they operate.

With an IT organization that’s very focused on development and technology innovation, how are people in their roles organized to be able to check and double-check code for vulnerabilities or use automated controls and approaches to protect those vulnerabilities?

Proper change management is essential. Before pushing code into production, security checks are made or application changes are evaluated for security-related vulnerabilities. Good training is an important start to improving prevention capabilities, though ultimately, security controls should be so robust that the employee rarely has to even think about it.

One recent Accenture initiative in Brazil assigned a team to identify potential vulnerabilities in different mobile devices. They looked at each of the banking applications that could be downloaded, and they were able to use a system that showed many vulnerabilities that existed in those applications.

Detection:  
How do we monitor?

Detection includes tools and metrics to identify and log aspects to manage operations. It also includes operational monitoring—aligning the tools to identify and detect threats along with their escalation and oversight.

As currently structured at most firms, surveillance is a reactive process using tools that look at past patterns to determine if a breach has occurred. For surveillance to realize its full potential as part of cyber resilience, it should become more proactive. Data from surveillance can make addressing identified vulnerabilities more proactive instead of waiting for an event to occur. We believe that a planned, systematic approach to investing in surveillance capabilities could generate significant returns, not only in terms of preventing and reducing adverse events, but in demonstrating a firm’s commitment to being a stable, dependable business partner.

Firms should consider using advanced data analytics—harvesting information from new channels such as social media and their existing channels such as transaction monitoring—to help create more predictive capabilities. Firms should be able to help prevent breaches in areas identified as having a high potential for undesirable activity. Ideally, firms should be able to turn post-event investigative data and tools into preventative detection systems that utilize analytics and real-time reporting to spot deviations from behavioral norms as they occur.

Using these methods, firms could also help create increasingly sophisticated risk profiles as they attempt to pre-empt breaches. In our experience, the total cost of investing time and resources in comprehensive, preventive surveillance is often less than the cost of investing in disconnected, group-by-group efforts; and the results are usually better. Most banks have separate efforts in place for employee surveillance, conduct risk and cyber risk. This could be an area to combine forces and seek better results with fewer gaps, and without needing additional funding.
Response:
How do we respond?

In the event a cyber attack occurs, firms should have in place an event response plan—the structure to identify and manage action plans—as well as a crisis management process to manage incidents and notify impacted parties.

A response plan includes:

1. Validating that the event is taking place and mobilizing the response team.

2. Putting in place the firewalls and stopgap measures to make sure the exposure isn’t expanding. This requires pre-planning and regular testing.

3. Determining the timing for alerting authorities and regulators, as well as the firm’s external media team.

4. Carefully managing public relations. Some firms have appeared stronger and more organized after a breach. Others have lost significant brand value.

A firm’s structured approach to cyber risk analysis should span each of the lines of defense to identify the risk components and aspect of change necessary to provide better clarity to key stakeholders. For example, scenario-driven impact analysis is one important technique. This involves conducting a tabletop scenario analysis workshop to re-evaluate the financial services firm’s response program in the event of a cyber breach, in light of heightened regulatory and management concern around cyber security.

The ability to quickly quarantine affected applications, networks and systems is also an essential part of the response plan. Based upon business case scenarios, firms should conduct business and technology resiliency tests to prepare for known and unknown situations which can occur in the case of situations which require a lockdown. They also need to be able to isolate technologies and platforms that are more susceptible to vulnerabilities and losses.
Making your Enterprise Cyber Resilient
Foresight

Resilience
Conclusion

Financial services organizations need to recognize the threats of cyber risk in a different way. Many have put in place thick walls to protect themselves.

But the threats from a cyber event are becoming more prolific. So, although the walls are in place, the threats or activities to commit fraud or attack a firm are evolving to evade traditional measures of protection.

Organizations cannot protect themselves at all times from the myriad of potential attacks through multiple channels. So putting in place structures, technologies and processes to build resilience—or fast recovery—is critical to operating effectively in today's connected world.
References


2. Ibid.


5. Ibid.


About the Authors

Steve Culp
Steve is a Senior Managing Director, Accenture Finance & Risk Services. Based in Chicago, Steve has more than 20 years of global experience working with clients to define strategy, and execute change programs across a broad spectrum of risk management and finance disciplines. Steve is responsible for leading the global group across all dimensions, from setting the strategic direction through to the enablement of local teams operating across diverse markets. In addition, he oversees Accenture’s efforts on large-scale transformation programs across finance and risk for some of our most important financial services clients.

Prior to his current role he was responsible for our Global Risk Management Practice, and prior to that he led Accenture’s Finance & Enterprise Performance consulting services for global banking, insurance and capital markets institutions. With his extensive experience in the financial services industries, combined with his knowledge of risk management and the finance function, he guides executives and client teams on the journey to becoming high-performance businesses.

Chris Thompson
Chris is a Managing Director, Accenture Finance & Risk Services, Capital Markets lead. Based in New York, Chris specializes in complex, large-scale finance and risk programs. He works with some of the world’s leading retail, commercial and investment banks. Chris brings 20 years of broad-based experience in financial architecture, risk management, performance management and trading to organizations determined to become high-performance businesses.

Jon Narveson
Jon is a Managing Director, Accenture Finance & Risk Services. Based in Charlotte, he serves as the Operational Risk Management Capability lead for North America specializing in risk identification, assessment, measurement, and reporting. Jon works with major financial services institutions to develop risk-based strategies, controls and risk mitigation programs to manage high impact and emerging risks and issues. His recent focus has included transforming operational risk management capabilities into drivers of value, profitability, and sustainability while strengthening the methods by which the risks are managed.
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 more than 358,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is www.accenture.com.

Disclaimer:

This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

Copyright © 2015 Accenture
All rights reserved.

Accenture, its logo, and High Performance Delivered are trademarks of Accenture.