

# *fs viewpoint*

[www.pwc.com/fsi](http://www.pwc.com/fsi)

3

Point of view

9

Competitive  
intelligence

14

A framework  
for response

22

How PwC  
can help

25

Appendix

## ***Threat smart:*** Building a cyber resilient financial institution



**pwc**

## Executive summary

Financial institutions have been addressing information security and technology risks for decades. However, a proliferation of cyber events in recent years has revealed that the traditional approach is no longer sufficient.

### What is cyber risk management?

*Cyber risk management is the coordinated management of intelligence, technology, and business operations to effectively manage an organization's business information assets to prevent unwanted consequences. It is the process by which a business protects its critical assets and reputation from external and internal threats from individuals or organizations, but it is not limited to technical measures. Increasingly, financial institutions should now see cyber risk management as an integral aspect of managing their business and controlling risks.*

### Cyber risk is more than an IT issue; it's a business issue.

While information security risks have dramatically evolved over the past few decades, the approach that financial institutions use to manage them has not kept pace. In our view, the traditional information security model — one that is controls and compliance based, perimeter-oriented, and aimed at securing data and the back office — does not address the realities of today.

Cyber risk management is a complex problem, requiring executive management engagement, ongoing governance, risk management techniques, threat correlation, collaboration throughout the organization, and adoption of a new business operating model. The ultimate objective of cyber risk management is to build cyber resiliency, where an organization's systems and operations are designed to detect cyber threats and respond to cyber events to minimize business disruption and financial losses.

### Building a robust cyber risk management program is a complex but worthwhile endeavor.

A cyber risk management program should be one of many components of your overall business risk environment that feeds into the enterprise risk management framework. While this doesn't eliminate cyber risks, it allows you to manage those risks through an informed decision-making process.

The executive management team should recognize its leadership role in setting the proper tone and structure for enabling cyber resiliency throughout the organization. They should also recognize the importance of mitigating cyber risks as an essential task in maintaining the on-going success of their institution.

We recommend executive management take the following steps:

1. Establish cyber risk governance.
2. Understand your cyber organizational boundary.
3. Identify your critical business processes and assets.
4. Identify cyber threats.
5. Improve your collection, analysis, and reporting of information.
6. Plan and respond. This step should include developing playbooks, improving cyber intelligence gathering techniques, leveraging cyber insurance options, and upgrading cyber security technologies.

### The benefits of becoming cyber resilient.

Cyber resilient organizations are better positioned to keep pace with evolving threats, thereby helping them to avoid financial damage, negative publicity, and loss of customers' trust.

---

## ***Point of view***

**Cyber risk is a business issue, not just a technology issue. Market leaders are finding that cyber risk management needs to be owned by the C-suite rather than by IT.**

***“The growing sophistication and frequency of cyberattacks is a cause for concern, not only because of the potential for disruption, but also because of the potential for destruction of the systems and information that support our banks. These risks, if unchecked, could threaten the reputation of our financial institutions as well as public confidence in the system.”<sup>1</sup>***

***—Sept. 18, 2013. Thomas Curry,  
US Comptroller of the Currency***

#### **A new day, a new reality.**

Financial institutions are increasingly vulnerable to incoming cyber security threats from new directions and adversaries. Attacks in the form of “hacktivism,” corporate espionage, insider and nation-states’ threats, terrorism, and criminal activity can cost an organization time, resources, and irreparable harm to its reputation.

The information security environment continues to change. In our view, financial institutions should ensure their cyber risk strategy addresses the following:

- Highly skilled, elusive threat actors.
- Cyber campaigns that are scalable and easy to customize.
- A complex, digital, evolving environment.

#### **Executive teams and boards can no longer afford to view cyber security as merely a technology problem.**

Cyber security breaches not only impact an institution’s bottom line, but also its reputation, brand, and intellectual property. The traditional information-security model — being controls- and compliance-based, perimeter-oriented, and aimed at securing data and the back office — is simply not designed to address today’s increasingly sophisticated cyber attacks.

The cost of defending against cyber threats has also risen sharply as regulators are focusing on how well financial institutions are defending themselves against these threats.

<sup>1</sup> Office of the Comptroller of the Currency, “Remarks before the Exchequer Club,” September 18, 2013, [www.occ.gov](http://www.occ.gov), accessed June 18, 2014.

***Information security alone is not enough to safeguard your bottom line and protect your organization from cyber risks. Effective mitigation of cyber risks is an essential component in maintaining the ongoing success of an organization.***



#### **Why cyber risk management matters.**

Information security systems are often designed to meet minimum levels of regulatory or industry compliance, rather than to identify the risks to the business and provide appropriate safeguards. As a consequence, many financial institutions address their cyber security threats reactively, adapting to threats as they are identified. In our view, this approach does not lead to cyber resiliency and therefore should change.

An appropriate cyber risk management program should be one of many components of the institution's overall business risk environment that feeds into its enterprise-risk management framework. Cyber risks should be treated like other serious business risk issues and now are viewed as an inevitable cost of doing business in today's digital world.

#### **What it means to be cyber resilient.**

We consider institutions to be cyber resilient when they have a comprehensive, well-crafted, cyber risk management program in place — with management held accountable for the program's performance and results.

#### ***Questions to consider as part of a cyber risk management program:***

- Have we performed a cyber business risk assessment to identify our key business risks?
- How do we know where to invest to reduce our cyber risks?
- What would be the disruption to our business from a cyber attack? How would it affect our business, brand, and reputation?
- How much revenue would we lose if our business processes were impacted by a cyber event?
- Have we identified our most critical business assets and do we understand their value to our adversaries?
- Have we looked at the value of these assets and business processes through the lens of the various threat actors?
- Do we have a cyber incident capability that will allow us to quickly respond to a cyber attack?
- How do we establish cyber risk tolerance to the organization?
- How do we communicate about cyber risk to the board and other stakeholders?
- Is my business resilient enough to survive a cyber attack?

***In our view, the executive team should provide leadership to achieve cyber resiliency, setting the proper tone and structure for the program.***



**The executive team should lead the transformation from the status quo of today's security program to one of cyber resiliency.**

To avoid potential damage to a financial institution's bottom line, reputation, brand, and intellectual property, the executive team needs to take ownership of cyber risk. Specifically, they should collaborate up front to understand how the institution will defend against and respond to cyber risks, and what it will take to make their organization cyber resilient.

To make this adjustment, market leaders are transforming their organizations from ones that are centered on security and technology to ones that combine these with business management, risk disciplines, and cyber threat expertise. By becoming cyber resilient, an organization is able to plan for, and mitigate, cyber risks according to its appetite to withstand disruption and financial loss.

**The executive team should also take the lead in setting the proper tone and structure.**

- The C-suite should recognize the importance and nature of mitigating cyber risk as being essential to the institution's ongoing success.
- The executive team should ensure that a program exists within the organization to manage cyber risks to reduce potential harm to their business and improve their cyber resiliency.
- Management of cyber risk requires direction from business-operations leadership at a level that can commit and command the resources required to address and respond to these challenges.
- It is essential to re-evaluate cyber risk priorities and investments to ensure that the financial institution's cyber business risk perimeter is fully protected.

## Executive management should take action to build their cyber risk management program.



We recommend executive management take the following steps:

- 1. Establish cyber risk governance** – The foundation of a strong cyber resilient organization is a governance framework for managing cyber risks. This is established by deciding who will be on each of the teams, and setting up operating processes and a reporting structure. Connections should also be made to other risk programs such as disaster recovery, business continuity, and crisis management.
- 2. Understand your cyber organizational boundary** – An organization's cyber vulnerabilities extend to all locations where its data is stored, transmitted, and accessed — by employees themselves, its trusted partners, and its customers. Organizations should also consider new areas such as big data, analytics, and social media.
- 3. Identify your critical business processes and assets** – Organizations should determine what comprises their most valuable revenue streams, business processes, assets, and facilities. We refer to these collectively as “crown jewels.” After these are identified, understand where they are located and who has access to them.
- 4. Identify cyber threats** – Effective cyber risk monitoring focuses on building a sustainable and resilient approach to putting intelligence inputs from various teams under a common lens to quickly correlate threats in real time. Financial institutions should establish a robust threat-analysis capability built on shared intelligence, data, and research from internal and external sources.
- 5. Improve your collection, analysis, and reporting of information** – Financial institutions should ensure their cyber risk operations team supports three primary functions to build robust cyber and technical threat intelligence capabilities. These are: collection and management, processing and analyzing, and reporting and action.
- 6. Plan and respond** – The development of prepared responses — playbooks — is a necessary step in adequately planning and preparing responses to cyber events. Using the intelligence gathered throughout the playbook development process, each playbook says who should take action, what their responsibilities are, and exactly what they should do. Executive management should also frequently revisit cyber intelligence gathering techniques, leverage and update cyber insurance options, and upgrade cyber security technologies.



***Building a robust cyber risk management program is a complex, but worthwhile endeavor.***



**The adversaries of today are quite different from those of the past.**

Formerly motivated by notoriety, technical challenge, and personal gain, yesterday's adversaries were focused on launching one-off attacks. Today — driven by economic, monetary, or political gain — well-funded adversaries are not only capable of organized, sustained attacks, but also are constantly developing new tools with which to assail their targets.

**Potential barriers on the road to success.**

As beneficial as the transformation from the status quo can be, we have seen organizations encounter multiple roadblocks en route to the desired state of cyber resiliency. And, as with any change initiative, institutions will likely be challenged by organizational and people issues, particularly those around remuneration and incentives. With an appropriate focus on the benefits of getting it right, these obstacles can be overcome.

**Adopting our cyber risk management framework enables an organization to become cyber resilient.**

Cyber resilient organizations are well positioned to keep pace with the changing threat landscape — spotting and thwarting threats on the horizon to keep critical assets and intelligence from falling into the wrong hands. This not only serves to avoid financial damage, negative publicity, and loss of customers' trust, but can also help prevent class-action lawsuits given that cyber breaches can be seen as evidence of negligence.

Effective implementation of our cyber risk management framework can also help financial institutions position themselves to gain a competitive advantage over their more vulnerable competitors that have opted to stick with the status quo.



---

## ***Competitive intelligence***

*Our observations of  
industry practices.*

**Information security monitoring is often focused on reacting to cyber threats in isolation, without realizing the threat to the financial institutions' finances and reputation.**



**Most financial institutions lack a program to manage cyber risks appropriately. We largely attribute this to the following:**

---

**Cyber risk management issues we've observed**

---

**Cyber threats viewed solely as an IT issue rather than a business issue**

In most financial institutions, cyber threats are managed by IT. However, in the new reality, the damaging consequences of poor cyber risk management spill over to impact the entire business.

**Lack of common processes and methodologies**

A financial institution's threat-monitoring and analysis activities are often disjointed, (for example, spread across multiple locations, maintained by different internal and external organizations, and hosted on multiple systems). This inhibits the ability to gather and manage cyber risk intelligence so as to recognize and rapidly respond to new threats in an evolving cyber security landscape.

**Cyber risk flying below the radar**

While many financial institutions have processes and controls in place to manage day-to-day risks, they often do not address cyber risks. These two types of risk share similar traits; both are hard to quantify, seem remote, and have a low probability of occurring. Typically, data-security systems are designed to meet just minimum levels of regulatory or industry compliance, rather than to identify the risks to the business and implement appropriate safeguards. Such institutions are ill-prepared to anticipate cyber threats and prepare a response in advance. They can only react.

**Inability to look at the big picture**

Existing information-security monitoring is largely focused on identifying and reacting to cyber threats in isolation. Traditional tools are only capable of identifying specific unusual patterns or traffic types and alerting operational teams when something outside the norm is happening.

**Reluctance to share cyber security intelligence**

When things go wrong, responses typically only address the specific problem at hand. Few attempts are made to see if similar problems are occurring in other parts of the organization. Often, organizations' cyber defenses rely primarily on data generated by internal monitoring rather than by reaching beyond enterprise boundaries to share insights and experiences.

**Taking a one-size-fits-all approach**

Many financial institutions do not consider the value of different assets when planning their cyber risk management strategy — making it difficult to set priorities regarding the investment of resources.

---

***Recognizing that cyber risk can't be completely eliminated, we see market leaders deciding on the level of cyber risk they are willing to accept, and then building their defenses around those parameters.***

Once agreement has been reached on where efforts should be focused, market leaders are taking steps to make their organization cyber resilient.

---

#### How leaders are addressing cyber risk issues

---

##### **Cyber threats viewed solely as an IT issue rather than a business issue**

Rather than having IT manage cyber risk, market leaders hold the CEO and board of directors accountable. Business lines and risk management play a key role in identifying and classifying information assets.

##### **Lack of common processes and methodologies**

We see leading financial institutions establishing programs that integrate processes, technologies, and risk methodologies into an enterprise-risk management program that manages cyber business risks in line with their risk appetite.

##### **Cyber risk flying below the radar**

Rather than taking a defensive posture, market leaders are being proactive in identifying, planning for, and mitigating the cyber business risks that are most likely to impact their organization.

##### **Inability to look at the big picture**

Leading financial institutions are transforming their organizations from ones that are centered on security and technology to ones that combine these with business management, risk disciplines, and cyber threat expertise. As they become cyber resilient, the organization is able to plan for, and mitigate, cyber risks according to its appetite to withstand disruption and financial loss.

##### **Reluctance to share cyber security intelligence**

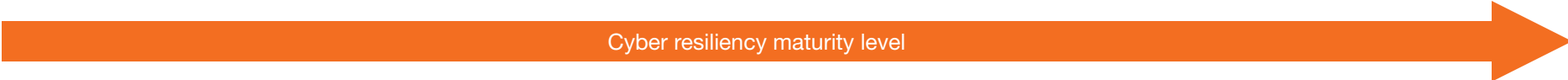
Market leaders establish open communication channels between corporate security, information security, threat management and analysis, law enforcement coordination, intelligence agencies, fraud, and operational risk to facilitate timely sharing of threat information with the right people to help mitigate the impact of cyber attacks.

##### **Taking a one-size-fits-all approach**


We have observed leading financial institutions building a cyber risk management program to protect their revenue streams, business processes, assets, facilities, brand, and reputation.

---

*We have observed financial institutions are at various levels of maturity when it comes to cyber resiliency.*

Cyber resiliency maturity level 			
Area of focus	Lagging	On par	Leading
Cyber risk governance	<p>The organization has limited insight into its cyber risk management practices.</p> <p>No one person or group is responsible for cyber risk governance.</p>	<p>The organization has established a threat-risk-response framework but does not view cyber risk governance as a competitive advantage.</p> <p>Leadership has a clear understanding of how cyber risks could impact their business.</p>	<p>Cyber risk governance is built into the organization's day-to-day activities.</p> <p>The organization has access to cyber expertise within its highest management levels.</p> <p>Leadership has a clearly defined action plan to respond to cyber incidents.</p>
Cyber risk perimeter	<p>The organization is unaware of where its data resides.</p> <p>There is little to no knowledge of third-party access to data.</p>	<p>Systems are designed to identify cyber threats at and within the organization's physical perimeter.</p>	<p>The organization's cyber risk management program includes all material third-party relationships and information flows.</p> <p>The cyber risk management program's perimeter includes trusted business partners, outsourced data centers, customers, and the cloud.</p>
Asset identification	<p>The organization does not differentiate between business and critical data.</p> <p>Access to data is not restricted to business need to know.</p>	<p>The organization understands the importance of its data and takes appropriate measures to protect it.</p> <p>Access to critical data is reviewed on an annual basis.</p>	<p>The organization knows what data is critical, where it is located, and who has access at all times.</p> <p>Leadership has a clear understanding of which assets are most critical to the organization and has looked at the value of these assets through the lens of the various threat actors.</p>

*We have observed financial institutions are at various levels of maturity when it comes to cyber resiliency.*

Cyber resiliency maturity level 			
Area of focus	Lagging	On par	Leading
Cyber risk monitoring	<p>Cyber threat monitoring is disjointed and ineffective.</p> <p>Responses to identified threats address little more than the specific problem at hand and are often quickly forgotten.</p> <p>Identified issues are not correlated to identify common threats.</p>	<p>Internal and external cyber risk assessments are performed on an annual basis.</p> <p>The organization takes a one-size-fits-all approach to monitoring its systems and data.</p> <p>Monitoring is designed to support a controls- and compliance-based security model.</p>	<p>Appropriate assessments of vulnerabilities to internal and external cyber risks are continuously performed.</p> <p>Common processes and methodologies are used to increase the organization's ability to gather and manage cyber risk intelligence.</p>
Cyber intelligence	<p>The organization's ability to consume intelligence is disjointed in nature and lacks common methods.</p> <p>Reported threats and attacks are not correlated between business groups.</p>	<p>Systems are in place but lack the ability to readily identify and respond to new threats.</p> <p>The organization is beginning to develop the capability to share intelligence, data, and research from internal and external sources.</p>	<p>Intelligence inputs from various functional teams are viewed under a common lens to quickly correlate and dynamically adjust the risk posture and respond to these threats in real time.</p>
Cyber risk management	<p>Senior management sees cyber risk as largely irrelevant.</p> <p>Leadership doesn't know who is responsible for managing cyber security incidents.</p>	<p>Management has set the proper tone for cyber risk management.</p> <p>The cyber risk management program is reviewed for effectiveness, but corrective actions are not always performed in a timely manner.</p>	<p>Leadership has taken full ownership of cyber risk management and understands its vulnerabilities, controls, and interdependencies with third parties.</p> <p>Employees demonstrate cyber awareness and the organization is seen as an industry leader in cyber risk management.</p>

---

## ***A framework for response***

*Our recommended approach  
to the issue.*

***Executive management should take action to build their cyber risk management program.***

An organization's cyber risk response is ongoing and iterative. The program evolves as the organization gains more insight into the nature, scope, and location of threats, and garners a better understanding of what it needs to protect and how.

Specifically, we recommend executive management take the following steps to protect their revenue streams, business processes, assets, facilities, brand, and reputation:

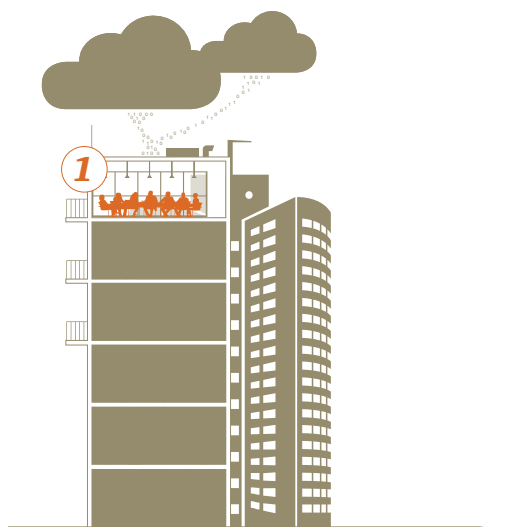
- 1. Establish cyber risk governance.***
- 2. Understand your cyber organizational boundary.***
- 3. Identify your critical business processes and assets.***
- 4. Identify cyber threats.***
- 5. Improve your collection, analysis, and reporting of information.***
- 6. Plan and respond. This step includes developing playbooks, improving cyber intelligence gathering techniques, leveraging cyber insurance options, and upgrading cyber security technologies.***





## Establish cyber risk governance

### Who will be responsible?



*The governance process should be designed to provide visibility to senior management and the board.*

*A cyber risk management capability should be a key component of the enterprise risk management program. This enables cyber risks to be managed through an informed decision-making process.*

The foundation of a strong cyber resilient organization is a governance process for managing cyber risks.

The governance process is established by deciding who will be on each of the teams, and setting up operating processes and a reporting structure. Based on our experience, three groups should be organized to carry out these efforts if these responsibilities aren't already assigned to existing groups.

Group	Key players	Responsibilities
Cyber risk governance committee	<ul style="list-style-type: none"> <li>Chief operating officer (COO)</li> <li>Chief risk officer (CRO)</li> <li>Head of security</li> <li>Heads of businesses and functional areas (such as business continuity planning, legal, risk/regulation)</li> </ul>	<ul style="list-style-type: none"> <li>Works with senior leaders to develop cyber risk strategy.</li> <li>Decides which information assets are essential.</li> <li>Sets the budget for cyber risk.</li> <li>Monitors the organization's cyber risk position and reports on it to senior leaders and the board of directors.</li> <li>Reviews reports from the cyber risk oversight and operations teams and helps prioritize emerging cyber threats.</li> <li>Revisits strategy to adapt the program as the cyber risk landscape evolves.</li> </ul>
Cyber risk oversight committee	<ul style="list-style-type: none"> <li>Information technology team</li> <li>Business support team</li> <li>Business teams</li> </ul>	<ul style="list-style-type: none"> <li>Assesses the active risks the organization faces, the people behind them, and the assets they threaten.</li> <li>Evaluates the effectiveness of the operations team.</li> <li>Identifies new threats and improves how information assets are protected.</li> <li>Determines how business changes affect the cyber perimeter — including new service offerings, suppliers, vendors, or business partners.</li> <li>Monitors status of patches and configuration changes to critical systems.</li> <li>Oversees employee training programs.</li> <li>Reviews new regulatory and compliance requirements.</li> </ul>
Cyber risk operations team	<ul style="list-style-type: none"> <li>Managers with operational experience of networks, information security, fraud, and corporate security</li> <li>Security operations center</li> </ul>	<ul style="list-style-type: none"> <li>Acts as first line of defense for detecting and responding to cyber events.</li> <li>Compiles real-time information from all the groups that monitor cyber threats.</li> <li>Produces reports for the cyber risk oversight and governance committees, including items such as: number and type of cyber events, origination and duration of events, which assets have been targeted, kinds of fraud attempted, comparison of cyber events to industry trends, incident and response reports, threat assessments, and intelligence reports.</li> </ul>

## Understand the cyber organizational boundary

What defines the boundary within which you will patrol?



*Decades ago, the cyber risk perimeter was limited to the data center. In the 1990s, the perimeter expanded to include connected terminals as the distributed computing model evolved. In the early 2000s, the perimeter further expanded to include third-party service providers that began to be integrated into the supply chain. With the now pervasive use of cloud computing, financial institutions today find themselves defending a perimeter which they can no longer completely see, control, or manage.*

### Understand the boundary that you need to protect.

An institution's cyber vulnerabilities extend to locations where its data is stored, transmitted, and accessed, both by itself and its third-party providers. The region that needs to be identified and understood is the cyber organizational boundary.

Any weakness in the perimeter becomes your vulnerability. This challenge will only increase as the organization's cyber security perimeter continues to expand as customers increase their demands for mobile tools that allow access to their information from wherever it resides to wherever they may be.

Key steps	Key considerations
Develop an enterprise level view of where critical assets and data reside	<ul style="list-style-type: none"><li>Putting equal priority on all of the data that the organization generates is not practical, cost effective, or necessary. Some of it is insignificant, but some is mission critical and will cripple the business if exposed.</li><li>Organizations should determine where their critical data stores are, where they are located at any given time, and who has access to them. This information can help develop a network perimeter. In addition to cloud, the evolution of big data, analytics, and social media have caused the boundary to be revisited.</li></ul>
Determine what systems and networks it traverses in supporting business operations	<ul style="list-style-type: none"><li>The perimeter extends far beyond the typical corporate network boundary to trusted business partners, outsourced data centers, customers, and the cloud.</li></ul>
Understand all the data shared with business partners, third parties, and "fourth parties" (third parties' data outsourcing and partnership arrangements)	<ul style="list-style-type: none"><li>Organizations should ensure they have the means and capability to have transparency into the cyber organizational boundary that extends far beyond the areas they directly control to wherever their critical information, data, and facilities reside. Any weakness in the perimeter becomes your vulnerability.</li><li>Organizations should enhance pre-employment due diligence for any insider who will have responsibility for IT operations, access to sensitive and protected data, responsibility for electronically transferring money, and other vulnerable functions.</li></ul>

## Identify critical business processes and assets

What items are critical to the survival of your organization?



Identify the assets you need to protect and the level of protection required for each.

Asset classification is not a new concept. In our experience, however, many financial institutions still struggle to get it right — organizations are over-protecting some assets and under-protecting others.

Organizations should determine what comprises their most valuable business assets, where these assets are located at any given time, and who has access to them. They should also determine which business processes, if compromised, would lead to significant hardship to the business. Finally, they should identify key facilities that house or support key data elements or business processes. We refer to these collectively as “crown jewels” — those information assets or processes, which if stolen, compromised, or used inappropriately would render significant hardship to your business.

Key steps	Key considerations
Identify critical assets and important business processes	<ul style="list-style-type: none"><li>• Crown jewels are those information assets or processes, which if stolen, compromised, or used inappropriately would render significant hardship to the business.</li><li>• Examples of crown jewels may include trade secrets, market-based strategies, trading algorithms, product designs, new market plans, or other business processes in addition to information assets.</li></ul>
Determine value of each asset and business process to the organization	<ul style="list-style-type: none"><li>• A “one-size-fits-all” model doesn’t apply when protecting key information. Financial institutions should hold business executives accountable for protecting the crown jewels in the same manner as they are accountable for financial results.</li></ul>
Define risk tolerance levels	<ul style="list-style-type: none"><li>• Financial institutions should define the right level of risk tolerance for their organization based on their business type. This will help determine the level of protection needed given their identified values and related risks.</li></ul>
Establish the levels of protection required for each asset type	<ul style="list-style-type: none"><li>• This would also include defining the ownership of risk for each asset, and establishing who within the organization can make decisions on accepting or mitigating risks related to them.</li><li>• Financial institutions can then prioritize their assets based on business risk.</li></ul>

## Identify, assess, and manage cyber risks:

### Cyber risk monitoring

How to build a sustainable and resilient approach.



#### Existing information security monitoring identifies and reacts to cyber threats in isolation.

Most information security tools are designed and implemented to identify specific unusual patterns or traffic types and alert operational teams that something outside the norm is happening. The responses address little more than the specific problem at hand and are often quickly forgotten. Few attempts are made to see if similar problems are occurring in other parts of the organization or if others are experiencing the same threats.

The typical IT-centric response is to deploy additional tools and personnel to somehow put it all together. While these tools can be quite useful in correlating known types of activities, they are incapable of automatically identifying and reacting to new threats. Effective cyber risk monitoring focuses on building a sustainable and resilient approach to putting intelligence inputs from various functional teams together under a common lens to quickly correlate and dynamically adjust the risk posture of the organization to these threats in real time.

Key steps	Key considerations
Bring together the various teams responsible for managing, tracking, and responding to cyber events	<p>This should include the following:</p> <ul style="list-style-type: none"><li>• Internal security operations center (SOC): IT operations team, systems for security information and event management (SIEM), and incident-response teams.</li><li>• Cyber risk governance: cyber risk governance committee, cyber risk oversight committee, and cyber risk operations team.</li><li>• Cyber threat intelligence can also provide valuable information to groups responsible for detecting fraud, money laundering, and terrorism financing.</li></ul>
Adjust cyber risk and control posture of the organization	<ul style="list-style-type: none"><li>• Adjust approach and perimeter as needed, depending on the location of assets, threat incidence, and state-of-the-industry landscape.</li><li>• Refine and update processes as necessary to adjust to evolving cyber risk landscape.</li></ul>

## Identify, assess, and manage cyber risks:

### Reporting and action

Improve your collection, analysis, and reporting of information.



### Turning threats into actionable intelligence.

Most organizations' threat analysis efforts inhabit a disjointed environment spread across several functions, physical locations, and systems. This disjointed nature and lack of common methods to consume intelligence is a significant barrier to establishing a robust cyber risk intelligence capability. To close this deficit, organizations should establish a robust threat analysis capability that is built on shared intelligence, data, and research from internal and external sources.

To build a robust cyber intelligence infrastructure, financial institutions should ensure their cyber risk operations team supports the organization by correctly analyzing cyber risk data, providing leadership with the cyber risk information it needs to make informed decisions, and proactively and quickly responding to attacks.

Key steps	Key considerations
Analyze cyber risk data	<ul style="list-style-type: none"><li>• Work out where threats are coming from, when they're happening, and what tools the attackers are using.</li><li>• Combine patterns you see from this analysis with knowledge of the business to give you a clearer picture of the threats you face.</li><li>• Tailor your monitoring systems, dedicating more resources where needed, and tuning them to react more precisely to the threats you face.</li><li>• Speed — both of processing cyber intelligence and reacting to it — is essential for combating the growing cyber threats you face.</li></ul>
Report to leadership	<ul style="list-style-type: none"><li>• Produce timely and meaningful reports for leadership, such as: the number and type of cyber attacks, the origination and duration of these attacks, which assets have been targeted, the types of fraud attempted, a comparison of cyber events to industry trends, incident and response reports, threat assessments, and cyber intelligence reports.</li></ul>
Proactively respond	<ul style="list-style-type: none"><li>• Take planned and rehearsed preventative measures to cyber attacks to shorten their duration and reduce the damage to the organization.</li></ul>

## Plan and respond: Start by planning for the inevitable.



### Prepare playbooks to respond to cyber events.

A strong governing team, with the right level of knowledge, expertise, and involvement at all levels of the organization is required to appropriately respond to cyber events. But waiting to prepare your response until after the cyber event has occurred is a recipe for disaster. The team must thoroughly understand the risks to their organization, the tools at their disposal, and their options in responding before a cyber event occurs.

The development of prepared responses — playbooks — is a necessary step in adequately planning and preparing responses to cyber events. Using the intelligence gathered throughout the playbook development process, each playbook says who should take action, what their responsibilities are, and exactly what they should do.

There are five steps for developing these playbooks:

Key steps	Key considerations
Devise scenarios	<ul style="list-style-type: none"><li>Think about the biggest cyber risks to your business and develop scenarios for some of the ways in which they're likely to happen. Each scenario should focus on a particular type of cyber attack and the assets it threatens. The scenario should also include the effects on your reputation, customers, finances, and your position with regulators.</li></ul>
Mitigate the effects	<ul style="list-style-type: none"><li>Decide which processes, tools, and techniques would be available to deal with the effects of the cyber attack in each scenario.</li></ul>
Develop incident response plans	<ul style="list-style-type: none"><li>What should your people do if an attack happens? Think about the people who own the information that's threatened. Also, consider each different part of the business — including corporate communications, media affairs, public relations, legal, marketing, law enforcement, and information technology. Write down the actions they should take, step by step, to get the business back to normal as quickly as possible.</li></ul>
Decide what extra resources you need	<ul style="list-style-type: none"><li>Define what you need to have ready — people, tools, or equipment — to deal with the effects of the cyber attack in each scenario.</li></ul>
Rehearse	<ul style="list-style-type: none"><li>Finally, get everyone to practice the responses set out in the playbook for each scenario. This gives people experience in dealing with cyber attacks, and makes them less disruptive and damaging. Having a documented, practiced response to each kind of attack will make your organization much more cyber resilient.</li></ul>

As the cyber risk management program matures, executive management should revisit playbooks, revise cyber intelligence gathering techniques, leverage and update cyber insurance options, and upgrade cyber security technologies.

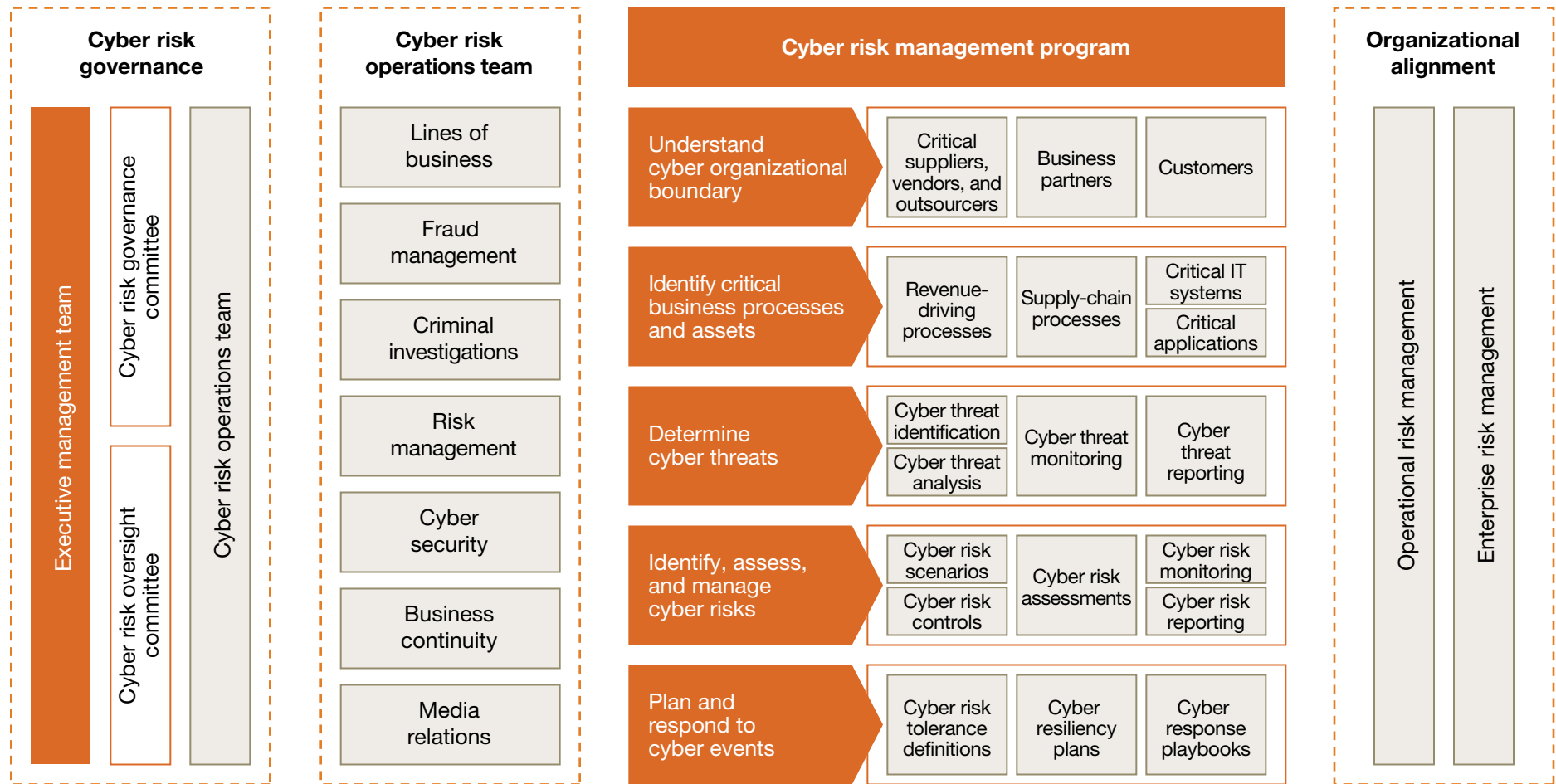
---

## ***How PwC can help***

*Our capabilities and  
tailored approach.*



**PwC can help your organization implement a roadmap for becoming cyber resilient.**



***We can help you across  
the spectrum of cyber risk  
management.***



<b>Cyber business risk assessments</b>	Organizations should identify cyber business risks by thoroughly scanning and analyzing all known and relevant risk factors, including those that have little likelihood of occurring. This provides a starting point for establishing an effective cyber risk monitoring and response strategy.
<b>The cyber risk management framework</b>	PwC assists in building or enhancing your cyber risk management framework, which includes understanding your cyber organizational boundary, identifying the organization's critical business processes and assets, understanding the scope of the organization's vulnerabilities, turning these threats into actionable intelligence, and responding with a continuous and process-oriented approach.
<b>Risk tolerance decision making</b>	Our advisors assist you in defining the appropriate level of risk tolerance for your organization based on its business type. This process includes defining the ownership of risk and establishing who within your organization can make decisions on accepting or mitigating risks.
<b>Protecting what's important</b>	PwC advisors assist organizations in determining what comprises their most valuable revenue streams, business processes, assets, facilities, brand, and reputation, identifying where they are located, understanding who has access to them, and establishing the levels of protection required by each asset type.
<b>Cyber risk monitoring</b>	We assist organizations in determining the types of monitoring systems required to support effective cyber risk management oversight, including providing assistance in installation and configuration of tools and dashboards, as well as the design of communication and reporting standards.
<b>Understanding the new cyber security perimeter</b>	Our advisors develop an enterprise-level view of where your data resides and what systems and networks it traverses in supporting business operations, including your shared data with business partners and third parties, as well as your data outsourcing and partnership arrangements (fourth party) to get a true picture of the scope of your cyber organizational boundary.
<b>Building cyber resiliency</b>	PwC can help you identify your "top ten" likely cyber events and build the playbooks needed to test and plan your responses. This includes establishing processes for continued re-evaluation of the top-ten list and revising/testing playbooks as your organization's environment and cyber threats evolve.
<b>Cyber risk dashboard and reporting</b>	Financial institutions need the right cyber risk management information at their fingertips to make informed management decisions. Our advisors can help you build the right cyber risk management reporting structure that has the right tools, content, and communication to meet your cyber risk management needs.
<b>Cyber risk response and remediation</b>	Following a cyber event, PwC is uniquely qualified to help organizations respond to cyber attacks. Our teams have deep forensic capabilities and can help you with post attack investigation, analysis, and remediation.

---

## ***Appendix***

*Select qualifications.*

## ***Assessment of potential weaknesses in cyber security system — Global financial services institution***

---

### **Issues**

The client's executives were concerned about the threat of cyber attacks that could result in the loss of critical data, reputational damage, and costly remediation. The client sought PwC's assistance to assess its cyber security system, identify its weaknesses, and implement measures to strengthen these defenses.

---

### **Approach**

PwC helped the client to identify areas in which it was vulnerable to attack, and to address these vulnerabilities in a strategic manner. Our approach included:

- Working with senior management to establish a cyber security strategy that would provide a wide-ranging defense against potential attacks.
- Assisting with the inventory of sensitive corporate data used by the client's business lines, and helping to determine if this critical information was stored securely.
- Using PwC's proprietary data-discovery methodology to determine the storage locations of data that might be of particular interest to attackers.
- Helping the client to perform in-depth, global assessments of its firewalls, proxy devices, servers, and other critical elements of its technology systems.
- Assisting the company in managing the configuration of about 400 firewalls, 50 proxy devices, and 8,000 servers to address concerns about inconsistent configuration.
- Assisting the client in performing an inventory of its end-user computing resources to establish where the system's weaknesses lay, and developing locked-down configurations for end-user workstations.

---

### **Benefits**

PwC's assessment helped the client to recognize that it needed a comprehensive cyber security system to replace its ad hoc approach. The critical asset inventory resulting from the engagement provided greater clarity about which assets required enhanced protection. The client also had a better understanding of where it was most vulnerable and which measures it could take to enhance its security. PwC's collaboration enabled the client to take a strategic approach to the challenge of safeguarding its assets, methodically identifying and addressing the risks it faced.

---

## **Forensic investigation and cyber security remediation in the wake of network attack — Global financial services institution**

---

### **Issues**

A major financial services company suffered a significant network intrusion involving its pre-paid debit card business. This resulted in financial losses as well as the compromise of sensitive client data and confidential corporate information. The intruders exploited a known vulnerability in the company's internet-facing system to gain access to its internal network. This reflected a serious deficiency in corporate governance. The client sought PwC's assistance to help establish and expand upon the findings of previous investigators, so the company could address concerns raised by regulators.

---

### **Approach**

PwC assisted the client by producing a detailed report outlining the nature, scope, and impact of the network intrusion. We deployed a large, multi-faceted team to provide forensic analysis, an assessment of the client's ongoing cyber security needs, and leading practices on cooperating with federal regulators. Our approach included:

- Assisting the client by developing an effective governance and project structure to manage a complex investigation involving multiple stakeholders.
- Performing a risk analysis of the company's compromised systems, and identifying more than 100 priority systems that needed to be imaged.
- Analyzing vast quantities of data, technical information, and emails to develop an accurate understanding of the intrusion and any cyber security weaknesses exposed by this attack.
- Extracting and loading hundreds of millions of forensic artifacts into a link-analysis tool.
- Conducting informational and technical interviews with more than 100 individuals.
- Reviewing contents of clients' files, including sensitive data, and assessing the cyber security risks associated with each file.
- Determining the business and regulatory impact of data that had been compromised.
- Producing an extensive report that confirmed some findings of a previous investigation and contradicted others, while also providing fresh facts and insights.

---

### **Benefits**

PwC helped the client to understand the full extent of the network intrusion, its causes, and its impact. This threat-based analysis enabled senior management to identify, prioritize, and address ongoing cyber security risks facing the company. The client was able to enhance its policies and processes, including its preservation of evidence and its response to security incidents.

PwC's report equipped the company with the facts required to respond to regulators' concerns and communicate with impacted clients. The client also received guidance on ways to secure the company's technical infrastructure, creating a program that exceeds industry benchmarks.

---

## ***Response to fraudulent transfer of customers' savings by cyber criminals — Fortune 500 wealth management company***

---

### **Issues**

A Fortune 500 wealth management company noticed a spike in reported instances of online fraud related to its retirement savings plans. Several customers reported that their accounts had been taken over by hackers. The perpetrators arranged loans against the savings in these accounts and wired the amount of the loan to a third-party bank account. Using phishing and spear phishing schemes, the attackers succeeded in obtaining the account holders' personal login details.

---

### **Approach**

The PwC team assisted the client by performing an in-depth forensic analysis of these cyber incidents. We then worked with the company to help implement extensive changes in its approach to cyber security. Our approach included:

- Performing a computer forensics investigation that involved collecting more than 10 terabytes of digital evidence relating to these cyber incidents, including Web server logs, firewall logs, and intrusion-detection system logs.
- Applying PwC's proprietary Breach Indicator Assessment to analyze the client's 30,000-node IT environment. Our risk-based approach involved reviewing all of the company's external-facing Web servers and user workstations to determine if any Breach Indicators had been triggered on these systems.
- Analyzing log data using PwC's proprietary Online Behavior Analysis Tool. This enabled us to determine which IP addresses and browsers the criminals used and what actions they took after gaining illegal access to customer accounts.
- Recommending specific security controls that would prevent further online fraud based on the findings from the Behavior Analysis Tool.
- Assessing the business impact of the cyber attacks. PwC was able to identify the defrauded customer accounts and the source of fraudulent access. This helped the client to assess the legal risks it faced due to the privacy breach, and also enabled it to share crucial evidence with law enforcement.

---

### **Benefits**

As a result of this engagement, the client had a better understanding of how the security breaches had occurred. It was also able to enhance its ability to detect and respond to cyber fraud by implementing a series of significant changes in its use of technology. The client also developed long-term, sustainable strategies to combat online fraud, including the development of an in-house incident response process.

---

## ***Threat modeling assessment to align cyber security defenses with key threats — Large US bank***

---

### **Issues**

A large US bank sought to assess its ability to detect and defend against cyber attacks. The company had developed defenses that it believed were adequate. However, senior management asked PwC to perform an independent evaluation in order to identify potential chinks in this information-security armor.

---

### **Approach**

PwC assisted the client by assessing which of its critical assets were most likely to attract attackers. We then modeled different threats to these targets. This approach included:

- Identifying sensitive resources that would present attackers with an alluring target.
- Using our Threat Modeling Framework to model the potential threats to these critical resources. This framework involves an in-depth analysis of seven different layers of threats, including everything from attacks on the company's publicly-accessible perimeter security to threats against its local system security.
- Documenting the company's existing defenses against such threats, and identifying gaps within this security system.
- Aligning the bank's defenses to address common threats within the banking industry.
- Performing defense effectiveness testing to assess the client's readiness for attacks.
- Developing a remediation roadmap to address gaps in the company's defenses.

---

### **Benefits**

PwC's threat modeling capabilities enabled the client to attain an in-depth understanding of common threats within the banking industry, and to assess which of these threats posed a particular risk to the bank. The project left senior management with greater clarity about the strengths and weaknesses of their security approach, including defenses on which they were overly reliant. The client also received a clear roadmap of security measures that would align its defenses specifically with key threats that it faced.

---



**[www.pwc.com/fsi](http://www.pwc.com/fsi)**

---

*To have a deeper conversation,  
please contact:*

---

<b>Joseph Nocera</b>	joseph.nocera@us.pwc.com +1 312 298 2745
<b>Stephen Russell</b>	stephen.j.russell@us.pwc.com +1 203 539 3079
<b>Shawn Connors</b>	shawn.joseph.connors@us.pwc.com +1 646 471 7278
<b>Scott Dillman</b>	scott.dillman@us.pwc.com +1 646 471 5764
<b>David Burg</b>	david.b.burg@us.pwc.com +1 703 918 1067
<b>Julien Courbe</b>	julien.courbe@us.pwc.com +1 646 471 4771

---

*Follow us on Twitter @PwC\_US\_FinSrvcs*

---

We would like to thank David Miles for his significant contribution toward this publication.

## **About our Financial Services practice**

PwC serves multinational financial institutions across banking and capital markets, insurance, asset management, hedge funds, private equity, payments, and financial technology. As a result, PwC has the extensive experience needed to advise on the portfolio of business issues that affect the industry, and we apply that knowledge to our clients' individual circumstances. We help address business issues from client impact to product design, and from go-to-market strategy to human capital, across all dimensions of the organization.

PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms in 157 countries with more than 184,000 people. We're committed to delivering quality in assurance, tax, and advisory services.

Gain customized access to our insights by downloading our thought leadership app: PwC's 365™ Advancing business thinking every day.



"Threat smart: Building a cyber resilient financial institution," PwC FS Viewpoint, October 2014, [www.pwc.com/fsi](http://www.pwc.com/fsi).

© 2014 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

BS-14-0359