Insights on
governance, risk
and compliance

December 2014

Achieving resilience in the cyber ecosystem

Building a better
working world

> **"An attack on one is an attack on all."**
>
> *Ken Allan, Global Cybersecurity Leader, EY*

Contents

Introduction

Rise of the cyber ecosystem

Rapid advances in technology are transforming the ability of every individual and every organization to better collect, analyze, and use its information as never before. Integrated networks, fueled by the internet, have removed the historical barriers to productively sharing information, unleashing the capacity of technology to revolutionize our economic and personal lives.

This phenomenon has seen the rise of the ***cyber ecosystem***: a complex community of interacting devices, networks, people and organizations, and the environment of processes and technologies supporting these interactions.

The cyber ecosystem's ability to simplify the sharing of information is simultaneously its greatest benefit and its greatest threat. The vulnerability of private and valuable information to theft, alteration or destruction by criminals or other malicious actors continuously increases. Localized disruptions can rapidly trigger a cascading sequence of events that can cause widespread technology disasters across entire networks and communities.

We are all subject to the dynamic forces found in biological ecosystems. They dictate the rules by which living entities develop, mature and die. Likewise, both organizations and individuals are often unwillingly exposed to the pathologies and "contagion effects" that thrive in the cyber ecosystem.

The expanding cyber ecosystem requires organizations to transform their use of technology to maximize benefits. At the same time, they must develop ***cyber resilience***: the ability to powerfully resist, react to and recover from potentially catastrophic cybersecurity threats, and reshape their environments for increasingly secure, sustainable cyber operations. Cyber-resilient organizations do not just rely on traditional technology solutions (such as firewalls) and processes (such as user and access management controls) to achieve this journey. They also leverage exceptional resilience leadership, culture, networks and change readiness to create a sustainable advantage over other organizations, cyber criminals and other malicious actors.

While many security threats are assignable to human agency (e.g. acts of careless staff and cyber criminals), many continue to relate to natural disaster. Such events often cripple the physical critical infrastructure (e.g. data centres and telecommunication networks) upon which the cyber ecosystem depends. Cyber resilience considers not only the confidentiality and integrity of information, but also its availability. In dealing with increased cyber criminality, organizations must not ignore natural hazards. Disasters caused by hurricane, fire or flood can be just as unpredictable and devastating as malicious attack.

Cyber criminals are resourceful and will use any circumstance available to achieve their ends – including the temporary disruptions triggered by natural events. Organizations need to understand how these varied sources of threat can coalesce into potentially overwhelming threat combinations.

The real question to explore is not ***why*** organizations need to be resilient, but rather ***how*** they can achieve sustainable, resilient operations in the cyber ecosystem. They must decide if, and how, they will achieve their business outcomes within an ecosystem in which individual survival is never guaranteed. Cyber attacks will continue to happen and there are no easy solutions. Otherwise, organizations risk "eco-cide" – extinction" through a process akin to "natural selection," which has eliminated 99% of all species that have existed on earth.

> Traditional security measures are "necessary but not sufficient" for organizational survival in the emerging cyber ecosystem.

This report covers:

- The growing complexity and risks within the cyber ecosystem and need to transform traditional approaches to protecting the "crown jewels" of organizations' sensitive and valuable information
- Understanding what cyber resilience means and how it can be developed as an integrated, strategic capability of organizations that operate in the cyber ecosystem
- The advantages of adopting a cyber-resilient approach to information security through a range of potential solutions to achieve sustainable, resilient operations

Changing security needs in the cyber ecosystem

Traditional defenses against cyber threats

In the pre-cyber ecosystem context an organization's critical information largely resided "on premise." Where network connectivity existed with the outside world it was limited. Informational "crown jewels" such as valuable intellectual property or client-sensitive information were protected through isolation and obscurity. Critical data was typically stored in stand-alone internal databases and networks, safe from the prying eyes of cyber criminals.

Perimeter defense

In this context, it made sense to simply protect the (virtual) perimeter of the organization. Mechanisms that protected the integrity of access and egress of data through the organizational perimeter were identified, strengthened and enforced. These measures were appropriate for the circumstances in which they operated, in a pre-cyber ecosystem context.

Traditional perimeter defense relied on the ability to clearly define (and delimit) the "technology boundary" of the organization and the means of securing the information contained within it. A solution characteristic of perimeter defense is the *firewall*, providing a barrier between an external (i.e., "untrusted") environment (the internet) and an internal (i.e., "trusted") corporate network.

Defense-in-depth

Over time, organizations increasingly exposed the systems that contained their critical information to external networks through private networks and the internet. They realized that that this level of exposure meant that perimeter defenses came under increased attack. Once a threat had breached the perimeter, the organization was defenseless. Subsequently, organizations adopted a "defense-in-depth" security model, so that if the perimeter was breached, there were other layers of security to protect critical information from falling into the wrong hands.

The basic philosophy relied on the concept of providing security for information wherever it was used. This made more and more sense once the sharing of critical data with external parties (including business partners) became ubiquitous. The "crown jewels" were no longer found securely behind the organizational perimeter (physical or otherwise). Rather, they were found across a number of systems, and devices, shared between an organization, its business partners and sometimes its customers. This triggered the need for a different approach with security measures found across the boundary of the "extended enterprise." Traditional mechanisms like firewalls continued to be used. However, new methods were employed that aimed to better track and protect information as it moved across the traditional perimeter, such as data loss protection (DLP).

Limitations of traditional defense

Organizational boundaries still exist, along with technology environments in which critical information is stored or processed. Under these circumstances, both forms of traditional security described will continue to be relevant and meaningful. Organizations will need to continue to establish both perimeter security as well as "defense-in-depth." The important thing is that they do not simply put full faith in these approaches.

Importantly, we have found that even where organizations have established traditional security mechanisms, they are often insufficient to provide the level of security and control they require. Organizations increasingly understand that traditional, device and technology-centric security measures such as firewalls are not sufficient to provide security in the cyber ecosystem.

The cyber ecosystem approach

Unlike traditional security approaches, the cyber ecosystem approach acknowledges the need to protect the information that matters most, wherever it is, on the basis that the most valuable data routinely passes between organizations, across networks, in innumerable business-to-business (B2B) and business-to-customer (B2C) settings.

In seeking to protect this data, it takes an integrated approach to incident detection and response, leveraging more intelligent systems, networks and devices, as well as organizational responses – recognizing that "an attack on one is an attack on all."

Cyber resilience focuses on measures that an organization can take on its own to increase its security from external and internal threats – as well as those it can collaboratively develop with business partners and industry peers. These measures include "hard" measures (such as technical improvements to physical devices) as well as "soft" measures (such as formal communication networks to share security intelligence).

Research performed by the US Department of Homeland Security (DHS)[1] focuses on developing cyber ecosystem resilience through measures that are based on three core principles:

- **Automation**, enabling rapid incident detection and response
- **Interoperability**, enabling distributed threat detection across devices and agents
- **Authentication**, enabling trusted communication for automated collaboration in a secure manner

These varied responses are part of an increasingly sophisticated and mature set of security measures that the cyber ecosystem approach requires.

Insights on governance, risk and compliance

October 2014

Get ahead of cybercrime

EY's 2014 Global Information Security Survey 2014

EY

Building a better working world

In our most recent Global Information Security Survey, many organizations have indicated that their traditional security strategies are inadequate. For example, 47% of respondents indicated that they either do not have a breach detection program or have perimeter network security devices with no formal processes in place for response and escalation.

When it comes to adapting to a hyper-connected, cyber ecosystem context in which threat responsiveness is key, many organizations indicated that they are likewise underprepared. For example:

- 28% of respondents do not have a hierarchy of incident severity with which to assess incidents.
- 42% of respondents do not have a security operations center (SOC).
- Of those with a SOC, only 30% collaborate and share data with others in their industry.
- Of those with a SOC, only 24% have dedicated resources focusing on cyber-threat intelligence.

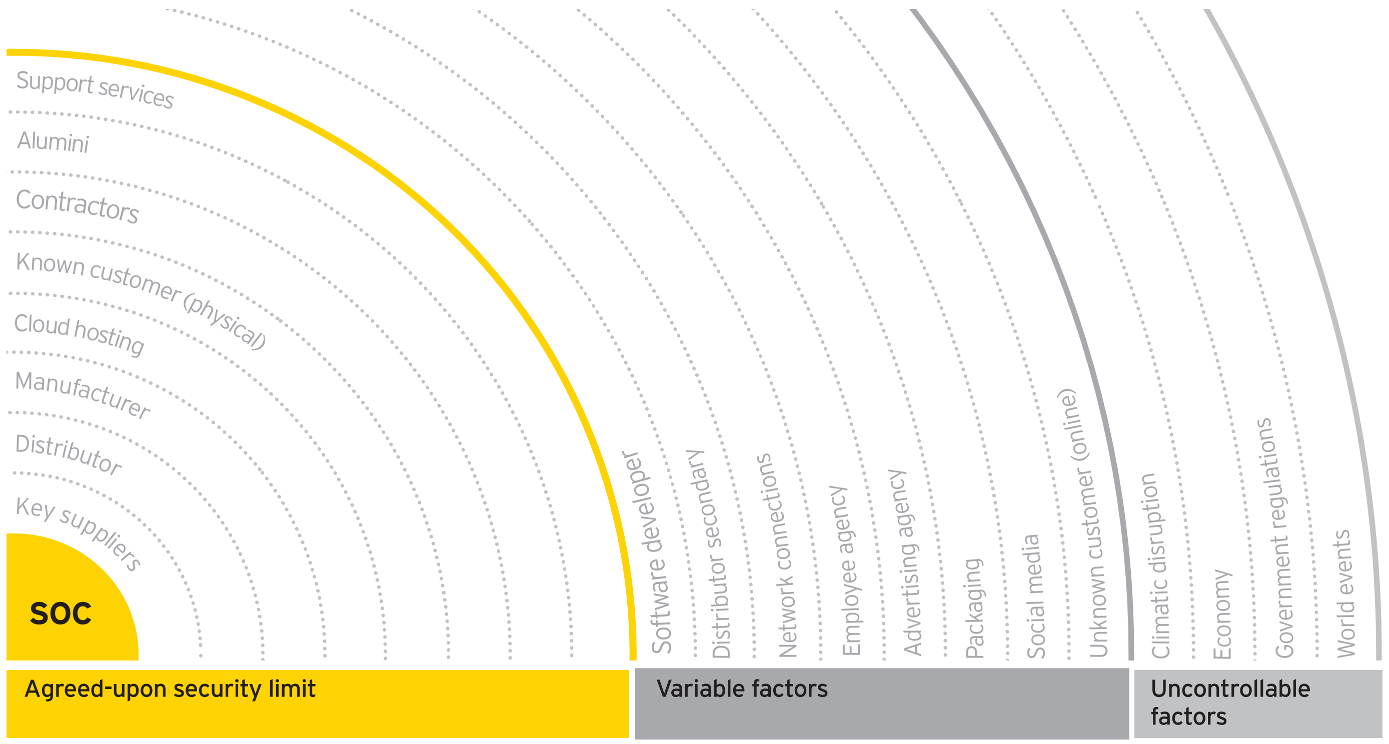
[1] *"Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action," US Department of Homeland Security, www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf, 23 March 2011.*

Implementing cyber resilience

Understanding your cyber ecosystem

The essence of managing risk in the cyber ecosystem is to understand that, unlike with traditional information security, it is no longer enough just to think about your own security. While still a good starting point, this approach to cybersecurity is insufficient for the extended enterprise. A cyber-resilient organization maps and assesses the relationships it has across the cyber ecosystem.

A typical business cyber ecosystem



Mapping the relationships
The first step in taking a cyber resilience approach is to understand how your organization is situated within the ecosystem. The organization must understand its internal and external environments and determine its "crown jewels" of information, where they exist and how they flow across this system. This allows the organization to take a risk-based approach, focused not on protecting all its information but on the information that is most critical to survival and growth.

An "agreed-upon security limit" can be established that sets out the key relationships with which the organization shares critical information to create value. The setting of a limit allows rules, guidelines and commonly accepted protocols for securing and sharing information between trusted parties. This is a key first step for an organization in establishing control over its cyber "neighborhood."

Determining the risk factors
The next step is to perform a risk assessment on the organization's "cyber presence" in the ecosystem, by looking at information assets, interdependencies with other organizations, threats (including insider threats), vulnerabilities, cybersecurity controls, and security testing activities, including business continuity/disaster recovery and reconstruction capabilities. This means examining those factors that affect the extent of the organization's control over its ecosystem and the means by which that control can be exercised.

These factors can be "variable", relating to exposures to the ecosystem or relationships that the organization can exert a degree of control over. For example, network connections and secondary distributors can have adverse impacts on an organization's cybersecurity, but they are at arm's length and often not pivotal relationships; options can exist to switch provider or reduce risky exposure if they present risks through their poor cybersecurity behavior.

"Uncontrollable" factors are events or potential threats that impact the cyber ecosystem and can have potentially catastrophic impacts on a wide range of organizations, not just single entities. Such risks are characteristically unknown or unknowable, and organizations must develop resilient cyber intelligence practices that are able to anticipate these factors as they emerge – and adjust security measures accordingly.

Establishing control in your cyber ecosystem
A detailed risk assessment will identify what risks exist across your cyber ecosystem and determine which security measures will provide you with control. In order to both establish these security measures and to assess the change in the status of risks you have identified, it is vital that the organization considers establishing a **security operations center** (SOC).

A well-functioning SOC can form the heart of effective detection. It can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively. A SOC can not only address security risks within an organization's traditional "perimeter" but also collaborate with trusted partners to build security across the wider ecosystem.

Taking a risk-based approach
Ultimately, establishing cyber resilience in the ecosystem is about instituting vigilance: systematically determining the extent and factors operating in an organization's cyber neighborhood. Threats constantly emerge, grow and are, in turn, replaced. It is vital that a central coordination team, through a SOC, provides an organization with the continuity of processes for monitoring, assessing and responding to the threats as they emerge on the horizon of the ecosystem.

With any risk-based approach that seeks to focus on tackling the "right risks" in the "right way," organizations must make tough, evidence-based decisions. Organizations must seek to take into account the connections, transactions and relationships that exist between entities within their cyber ecosystem.

They also need to decide what they are willing to manage within the boundaries of their defined ecosystem limits. Should the organization seek to control the risks faced by groups that are one step away (e.g., suppliers)? Or should they also try to influence risks faced by groups further from the center (e.g., the suppliers of suppliers)?

Within its defined ecosystem, organizations need to continually reassess relationships and risks, adjusting as the business evolves. Agility is needed to react to uncontrollable factors that affect every business in similar, but distinct, ways.

Organizations need to ask:

- How much can we do to manage the residual risk?
- Are we prepared to accept a certain level of risk?
- What can we attempt to control and what do we need to accept is out of our control (for example, world events and changes in location regulations)?

Attributes of a cyber-resilient organization

Managing the unknown and the unknowable

A key characteristic of the cyber ecosystem is that organizations are far more exposed to a wider range of unknown, or even unknowable, security threats. Attacks have become more sophisticated, and so-called "zero-day threats" have become commonplace. This unpredictability makes it ever more unlikely that a single approach, technique or device will provide the level of security that is needed. Unfortunately, there is no "silver bullet" that will ensure an organization's survival in the cyber ecosystem.

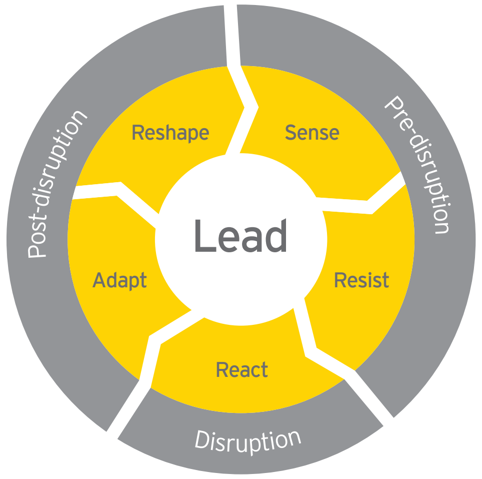
Given this dynamic, organizations must consider establishing the organizational functions (such as SOCs) that allow them to *institute vigilance* and to be able to respond flexibly to threats as they arise. This and other "hard" measures provide a basis for a coordinated and systematic approach. Beyond this, so-called "soft" measures are needed that seek to influence organizational behaviors. Behavioral attributes establish vigilance for threat detection and energize the vigor, focus and creativity required in successfully responding to and mitigating the impacts of security incidents.

Resilience attributes go far beyond simply purchasing and installing hardware and application device that "promise" security. They demand a focus on developing the "human element" in developing security, and they explicitly acknowledge the vital role that individuals, teams and relationships play in keeping organizations safe within their increasingly complex threat environments.

Understanding the "resilience cycle"
Organizations need to establish an understanding of the "resilience cycle" helping Information Security teams continuously build upon the experience of responding to threats.

This requires them to learn and adapt through the key resilience phases:

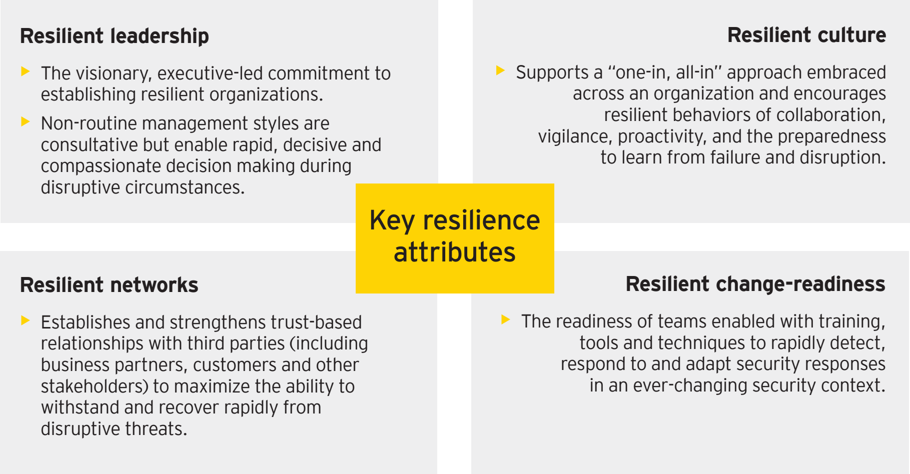
- During ***pre-disruption***, through an ability to better sense and resist security threats, including advanced capabilities to scan internal and external environments, and eliminate vulnerabilities
- During ***disruption***, by reacting rapidly to sudden events that threaten the organization; leveraging non-routine leadership and mobilizing effective responses that minimize impacts
- During ***post-disruption***, by absorbing shocks while continuing to achieve strategic security goals and reshaping and reconstructing the operating environment in ways that eliminate future sources of disruption threat



> *Resilience* is the strategic organizational capability to resist and react to disruptive and destructive threats, reshape environments, and survive both foreseen and unforeseen risks.

Developing resilience attributes

While certainly not easy to define or track as directly as investments in the latest security-related hardware, organizations should nevertheless aim to track and assess resilience attributes. These attributes provide a key element of the flexibility with which organizations that demonstrate the ability to "anticipate" security threats.



Key resilience attributes

Resilient leadership

- The visionary, executive-led commitment to establishing resilient organizations.
- Non-routine management styles are consultative but enable rapid, decisive and compassionate decision making during disruptive circumstances.

Resilient culture

- Supports a "one-in, all-in" approach embraced across an organization and encourages resilient behaviors of collaboration, vigilance, proactivity, and the preparedness to learn from failure and disruption.

Resilient networks

- Establishes and strengthens trust-based relationships with third parties (including business partners, customers and other stakeholders) to maximize the ability to withstand and recover rapidly from disruptive threats.

Resilient change-readiness

- The readiness of teams enabled with training, tools and techniques to rapidly detect, respond to and adapt security responses in an ever-changing security context.

Overcoming a "functionalist" approach

It has traditionally been all too easy to dismiss the need for a holistic, resilience approach to information security. It is always easier to reach for the checkbook in the hope that the next security hardware purchase will solve all the problems. Unfortunately, if that strategy ever really worked, the inexorable rise in security threats has proven that it is no longer enough. A cybersecurity strategy that focuses on the behaviors – not only of security teams but all employees – is vital.

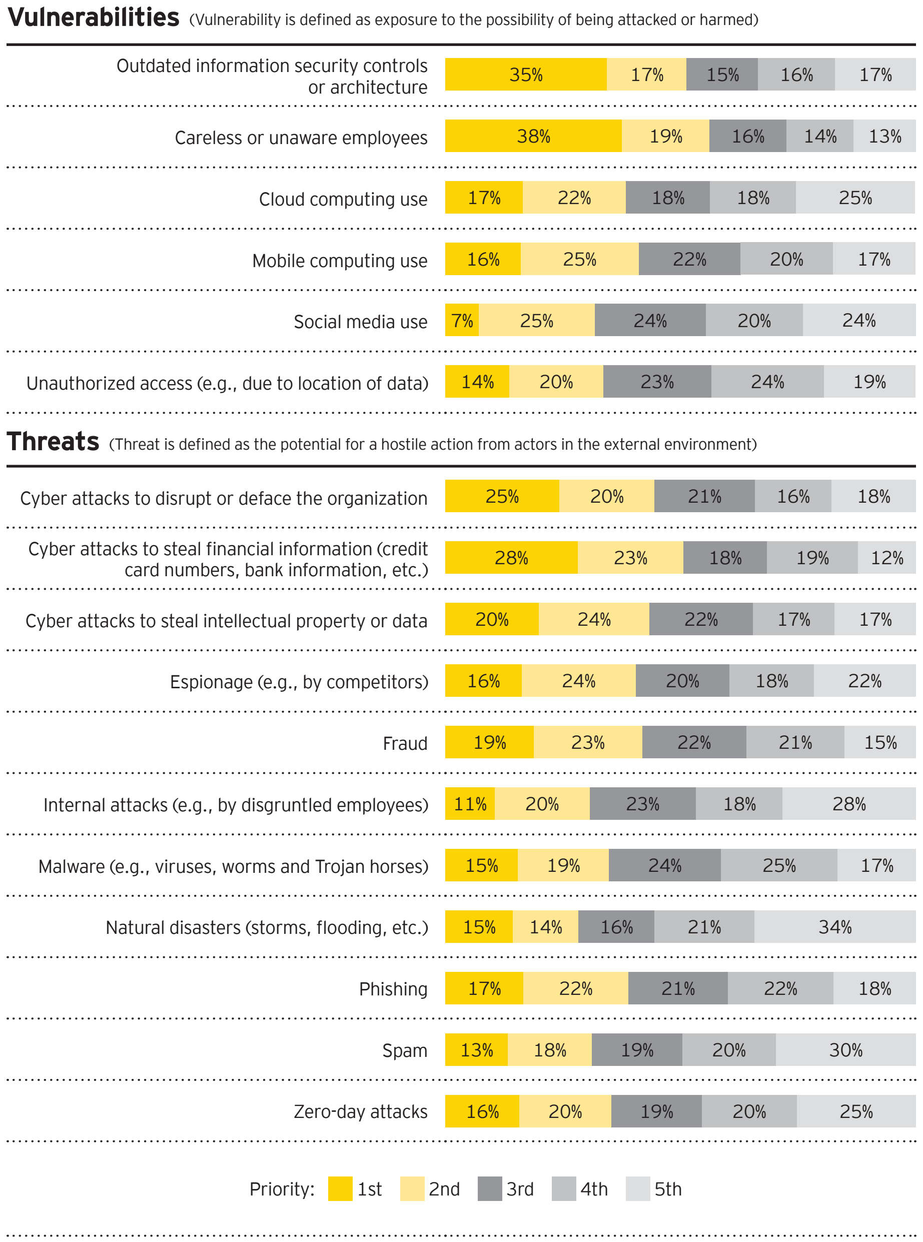
Leveraging resilient culture

The cyber ecosystem approach fosters a resilient culture by augmenting "command and control" security models, in which information security departments are charged with the entire responsibility for protecting the organization while the broader organization is less engaged, to one in which information security is seen as everyone's business. A resilient culture minimizes insider threat and encourages employees to identify and respond to vulnerabilities.

Leveraging resilient leadership

Government agencies are beginning to develop national policy frameworks that aim to provide a legal and policy foundation from which to implement a resilient cyber ecosystem. At the organization level, a key step forward is to have executives and boards committed to resident operations within the cyber ecosystem, and transparency is vital. Increased use of governance, risk and compliance (GRC) tools that improve the visibility of security vulnerabilities is assisting this.

Although by no means the only threat, the 2014 Global Information Security Survey demonstrated that the top vulnerability to organizations' security in the cyber ecosystem continues to be "careless or unaware employees."



Vulnerabilities (Vulnerability is defined as exposure to the possibility of being attacked or harmed)

Threats (Threat is defined as the potential for a hostile action from actors in the external environment)

Collaboration across resilient networks can help organizations anticipate and mitigate cyber attacks.

Leveraging resilient networks

By consolidating, correlating and cross-referencing logs across systems, organizations can establish baseline information indicative of "normal" system or network behavior. Then, by integrating this information with intrusion detection and response processes and technology, organizations can leverage automation to rapidly identify abnormal and potentially malicious activity.

Used judiciously, organizations should seek to leverage automation for real-time detection of attacks, supporting proactive responses to security threats. Tightly integrated cloud-based cyber intelligence services could help provide near real-time detection of advanced persistent threats (APTs) while leveraging trained users as "human sensors."

Leveraging change-readiness

Organizations need techniques and tools that allow them to respond with agility and adaptability to emerging threats and cyber attacks. There are many tactical approaches that can be used to drive this agile capability, including:

- Decentralized data protection built into, and as close as possible to, the information itself — for example, through capabilities such as innovative information rights management solutions where security controls are built into data files and communicate with them regardless of the storage or transfer medium
- Adaptive and decentralized intrusion detection and response built into devices and networks in a manner that matches their intended criticality and sensitivity
- Whole-of-system resilience built into devices and networks where they revert to a "trusted state" when faced with an advanced attack, or have a predefined life span
- Automated communications between devices and networks, enabling programmed and collective responses to abnormal or malicious behavior
- System-wide cyber attack sensors providing automated alerts with SOCs sharing information with government computer emergency response teams (CERTs), cybersecurity operations centers (CSOC), intelligence organizations and law enforcement

Expanding the radius of cybersecurity

Using cyber threat intelligence

In addition to deploying traditional security tools with an inward view of an organization's corporate network, an extended view should be considered of its external environment. Such consideration is key to cyber threat intelligence (CTI); through it, organizations are able to better understand the evolving cyber threat landscape as it affects their ecosystem.

CTI is an advanced process that enables the organization to gather valuable insights based on the analysis of contextual and situational risks which, gives it the ability to respond proactively to identified threats and can be tailored to the organization's specific threat landscape, industry and markets. CTI focuses on examining the information created and shared by the organization, how its products and services are developed and used, and the security risk context of its corporate strategy operating in the wider industry and geopolitical context.

However, CTI should not be used solely to prepare for attacks directed at a single organization. Organizations should seek to proactively collaborate with peers, clients, suppliers and the government. This helps industry bodies provide a unified front against cyber threats and avoid public mistrust of cyber services triggered by a lack of information about security issues. To achieve this, resilient networks with formal structure and near real-time communication need to be established with professional and coordinating bodies — for example, CERTs, CSOCs, International Information Systems Security Certification Consortium, and the Open Application Security Project (OWASP) — which increase the ability of organizations to learn from previous cyber attacks and adapt. It is important that these relationships are integrated into the cybersecurity strategies of organizations.

Most organizations do not sufficiently understand the security capabilities of their business partners.

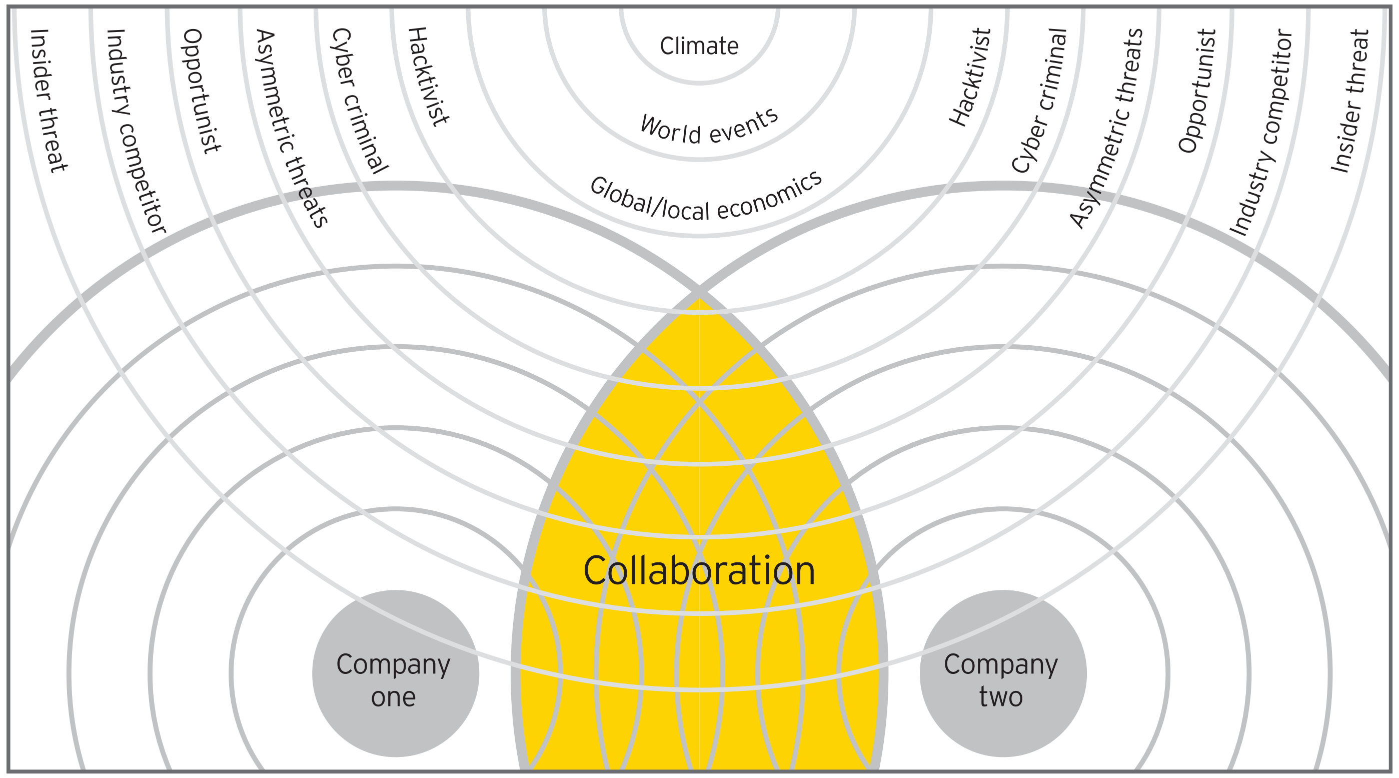
The most common third-party controls of respondents to the GISS 2014 were "security assessments performed by the client organization's security or internal audit function" or "self-assessments" performed by the third-party organizations.

Collaboration is vital

The sharing of information in a larger group, whether ad hoc, semi-formal or a moderated formal environment, is the key ingredient for organizations with the most success at understanding, scoping and mitigating intrusions in their networks. Organizations need to recognize the interdependent relationships they have in increasingly complex networks. Key relationships to consider should no longer be limited to "core" suppliers and business partners, but should include outsourcing providers, IT service providers and cloud service providers. Organizations should no longer just be concerned about the security capabilities of their direct suppliers, but they should consider the suppliers of those suppliers (and beyond).

Typically there is also a focus on requiring certifications and third-party independent assurance and on imposing contractual liability. Although this may reduce risk, unfortunately such controls do not prevent the impacts of cyber attacks, and a more collaborative approach is becoming increasingly necessary. Specifically, larger organizations should realize that their security capabilities will typically exceed those of their suppliers, and it can be beneficial to take some of the key members of the broader ecosystem under the "protective wing" of the stronger party. Intelligence sharing, shared SOCs and coordinated cybersecurity activities are examples of collaborative approaches that larger organizations can initiate, taking a resilient ecosystem view toward their supply and activity chain.

Potential collaboration within the ecosystem



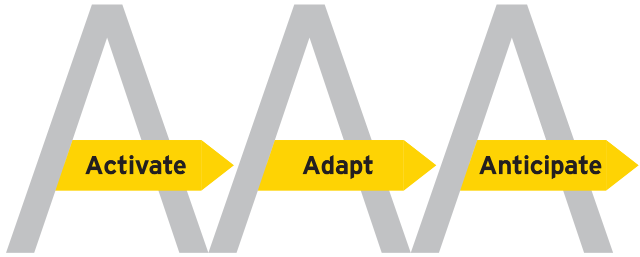
> Cybersecurity knowledge sharing, where properly established in secure and trusted environments, represents a significant "win-win" opportunity, advancing the interests not only of individual businesses but also for entire industries and the societies that depend on them.

However, organizations should be cognizant that not all efforts to embrace unified security systems will advance their interests or the interests of the whole. Unless properly implemented, enforced knowledge sharing and common processes can undermine, rather than improve, the cyber operations resilience of organizations operating independently.

Collaboration can be used to increase an organization's security posture and ability to proactively detect and respond to incidents. However, good collaboration will not work without strong cybersecurity defense channels in place – although this can be challenging to establish in the context of advanced persistent threats (APTs). These are often highly targeted, multi-layer attacks tailored for the intended victim; therefore, a specific attack may not necessarily be visible to competitors or other organizations. Further, APTs are no longer only driven by state agents: private organizations now sell advanced "offensive" services that other organizations can employ to gain competitive advantage over their competition.

Committing to the cybersecurity journey

To survive and thrive in the increasingly complex and risky cyber ecosystem, organizations must undertake a *cybersecurity journey*, transforming from being an "easy target" within the cyber ecosystem to becoming something more formidable.



This journey requires them to:

- **Activate** foundations of cybersecurity through developing a comprehensive set of information security measures to provide a basic defense against cyber attacks
- **Adapt** security measures to keep pace with changing business requirements and operating environments to establish a dynamic approach
- **Anticipate** and disrupt potential cyber attacks, proactively using robust and mature cyber threat intelligence, risk assessment, and incident response capabilities

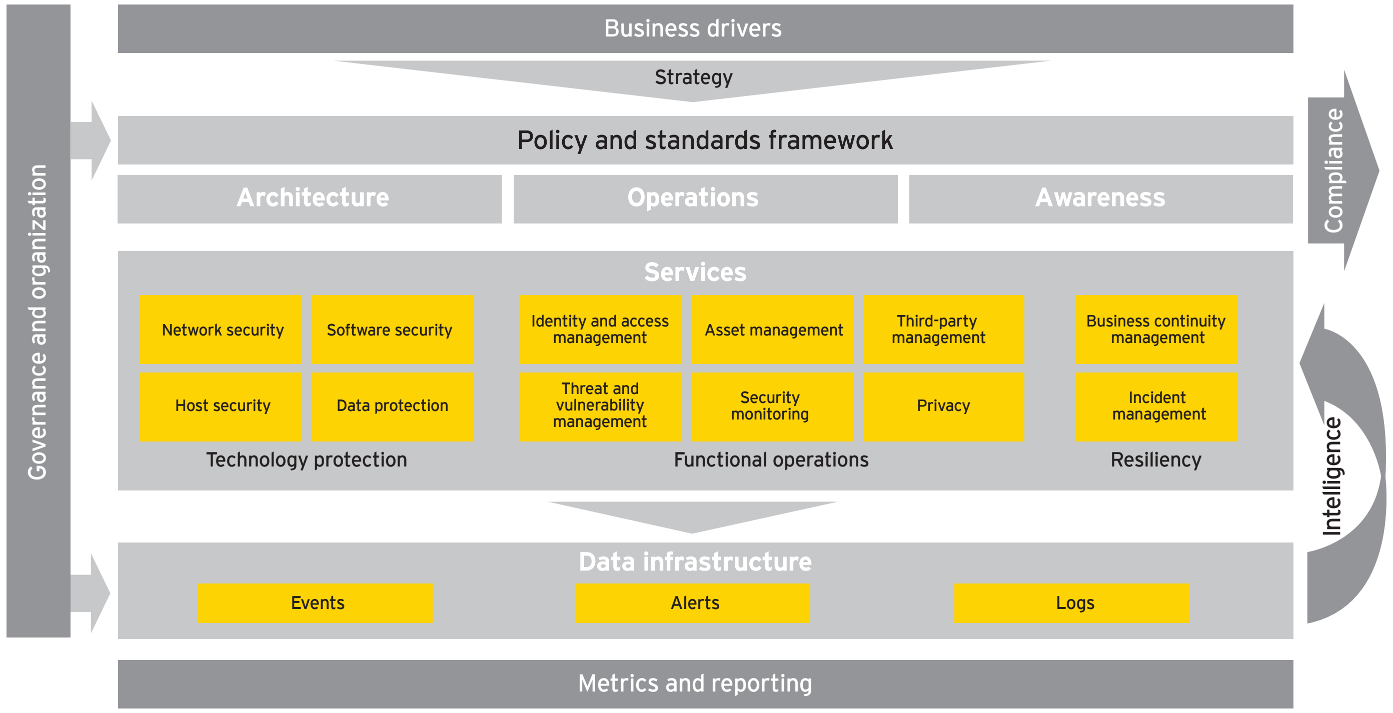
Organizations should work out where they are on their cybersecurity journey and determine what they need to do to advance their capabilities – the aim should be to implement ever more advanced cybersecurity measures at each stage. They must seek firstly to activate, then adapt and finally anticipate threats within their ecosystem – ultimately, anticipating cyber attacks is the only way to get ahead of cybercrime.

Cyber Program Management (CPM)

Organizations should consider establishing CPM, which provides a systematic, holistic framework for identifying and addressing security risks within the cyber ecosystem.

EY's CPM framework is aligned to International Organization for Standardization (ISO/IEC 27001:2013) and a meaningful analysis of how information security shapes and fits into an organization's overall risk management structure. At its foundation is a clear focus on the organization's strategic priorities and business objectives *(see figure below)*.

EY's CPM framework



Conclusion

The cyber ecosystem is evolving but not yet resilient

The question is not "why" organizations need to protect themselves in the cyber ecosystem. It is already a reality.

The real questions are: is your organization cyber resilient, and how can you achieve sustainable, resilient operations for the future?

In the evolving threat environment, traditional information security approaches will increasingly be seen as "necessary but not sufficient" to fully protect individual organizations. Organizations need to establish confidence in their base-level security maturity, but in doing so they need to recognize that they cannot thrive in business on their own.

Organizations need to invest not only in the right security technologies but in better understanding their ecosystem and working with trusted partners to further protect that ecosystem together. A resilient cyber ecosystem is a valuable goal that can provide the organizations operating in it with an increased confidence in the security of their systems and data.

Organizations should start to look beyond their own borders and begin to assess the impact of a cyber attack on their business partners, suppliers, vendors, etc. They should seek to be good "cyber citizens" in helping develop healthy, resilient cyber ecosystems with third parties they need to interact, communicate and share data with.

They need to increase the level of collaboration (rather than just monitoring) of their ecosystem, working more closely with others in the industry, competitors and governments to combat the threats that face them all as a team.

But cyber ecosystem collaboration requires more than words or written agreements scripted by legal and commercial teams. It requires a true commitment to cyber resilience and to enforcing the behavioral attributes of resilience leadership, partnership and change-readiness. Most of all, it requires the unwavering commitment of individuals and leaders.

Governments and major organizations are taking a leading role in establishing the policy and practice frameworks to develop resilient cyber ecosystems. This is an ongoing proposition that is gaining traction but is not yet in place due to the complexity involved. In the meantime, organizations should ensure they develop their own information security capabilities with sufficient maturity to address their individual risk contexts.

Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective. Please visit our *Insights on governance, risk and compliance* series at www.ey.com/GRCinsights.

Get ahead of cybercrime: EY's 2014 Global Information Security Survey 2014

www.ey.com/GISS

Cyber Program Management: identifying ways to get ahead of cybercrime

www.ey.com/CPM

Cyber threat intelligence – how to get ahead of cybercrime

www.ey.com/CTI

Security Operations Centers – helping you get ahead of cybercrime
EY

Security Operations Centers – helping you get ahead of cybercrime

www.ey.com/SOC

Privacy trends 2014: privacy protection in the age of technology

www.ey.com/privacy2014

Maximizing the value of a data protection program

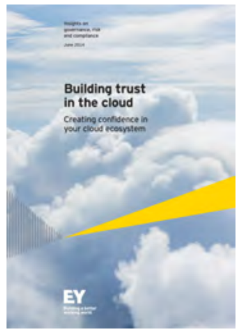
www.ey.com/dataprotect

Identity and access management: beyond compliance

www.ey.com/IAM

Big data: changing the way businesses operate

www.ey.com/bigdatachange


Building trust in the cloud
Creating confidence in your cloud ecosystem
EY

Building trust in the cloud: creating confidence in your cloud ecosystem

www.ey.com/cloudtrust

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. AU2822
ED None.

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights

About EY's Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or, more specifically, on achieving growth or optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view: ey.com/advisory

Our Risk Advisory leaders are:

Global Risk Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Area Risk Leaders		
Americas		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
EMEIA		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp

Our Cybersecurity leaders are:

Global Cybersecurity Leader		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Area Cybersecurity Leaders		
Americas		
Bob Sydow	+1 513 612 1591	bob.sydow@ey.com
EMEIA		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Asia-Pacific		
Paul O'Rourke	+65 6309 8890	paul.orourke@sg.ey.com
Japan		
Shinichiro Nagao	+81 3 3503 1100	nagao-shnchr@shinnihon.or.jp