

Security Program Management from a leadership perspective

GTA Technology Summit 2014

5 May 2014



Building a better
working world

Disclaimer

This presentation is proprietary to Ernst & Young LLP. Without Ernst & Young LLP prior written permission, this document, either in whole or in part, must not be reproduced.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither Ernst & Young LLP, EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this presentation. On any specific matter, reference should be made to the appropriate advisor.

Agenda

- ▶ Increasing cyber risk
- ▶ Cybersecurity from a business and organization leadership perspective
- ▶ What are organizations doing
- ▶ Questions

Increasing cyber risk



**“The question is not if
your organization will be
breached, or even when.
It has already happened.**

**The real questions are:
are you aware of it, and
how well are you
protected for the future?”**

Ken Allan
EY Global Leader, Information Security

Why cybersecurity matters

Cyber threats represent real risk to organizations and citizens

External attacks are increasing



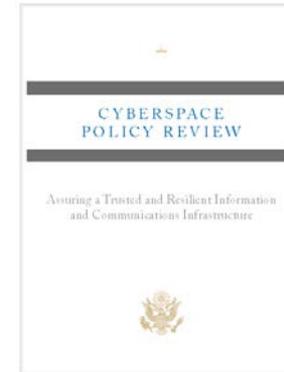
59% of respondents perceived an increase in the level of risk they face due to external threats.

Attackers are stealing sensitive business & customer data



"APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations."

Cyber attacks impact the bottom line



Between 2008 and 2009, American business losses due to cyber attacks had grown to more than US\$1 trillion of intellectual property.



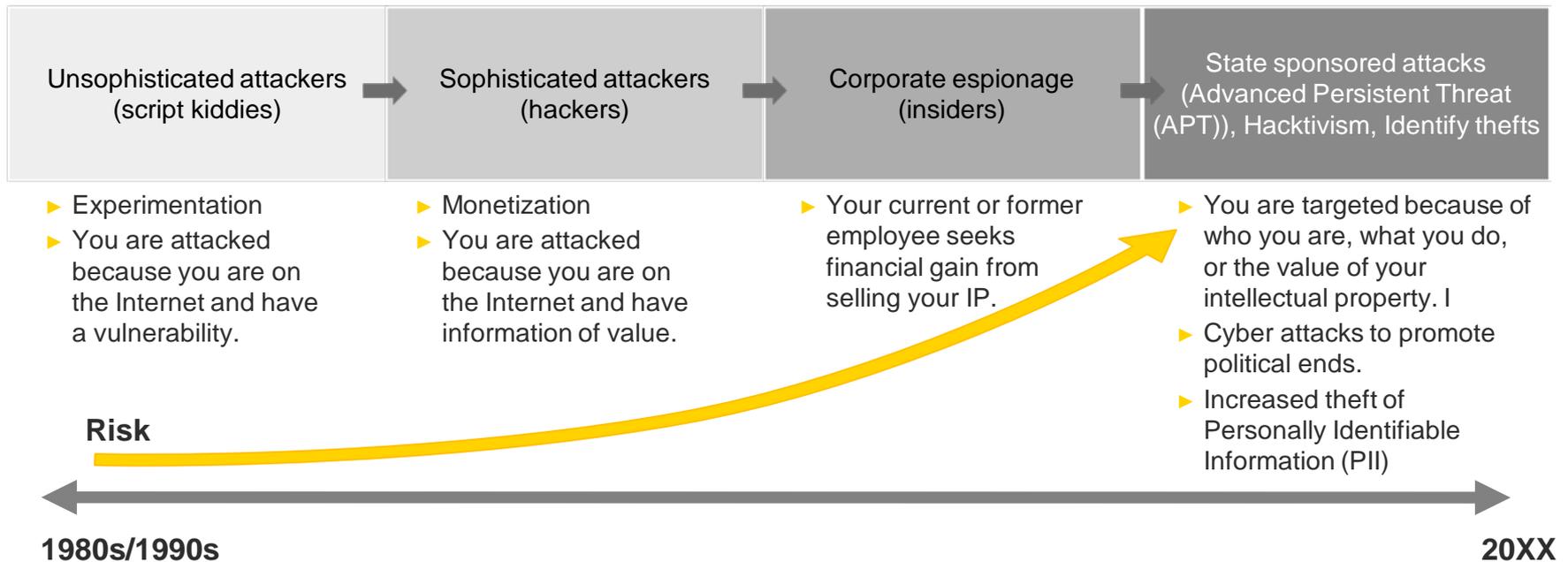
"92% [of data breaches] perpetrated by outsiders



State-affiliated actors tied to China are the biggest mover in 2012. Their efforts to steal IP comprise about one-fifth of all breaches in this dataset.

Cyber security threats are constantly evolving

Cyber security threats are constantly evolving, and target all types of organizations. **Attackers today are patient, persistent, and sophisticated, and attack not only technology, but increasingly, people and processes.** The challenges faced today that have altered expectations, strained resources, and caused a paradigm shift in information security processes.



Key findings in EY's Global Information Security Survey 2013

Key findings in EY's Global Information Security Survey 2013 reveal ominous causes for concern for the public sector:

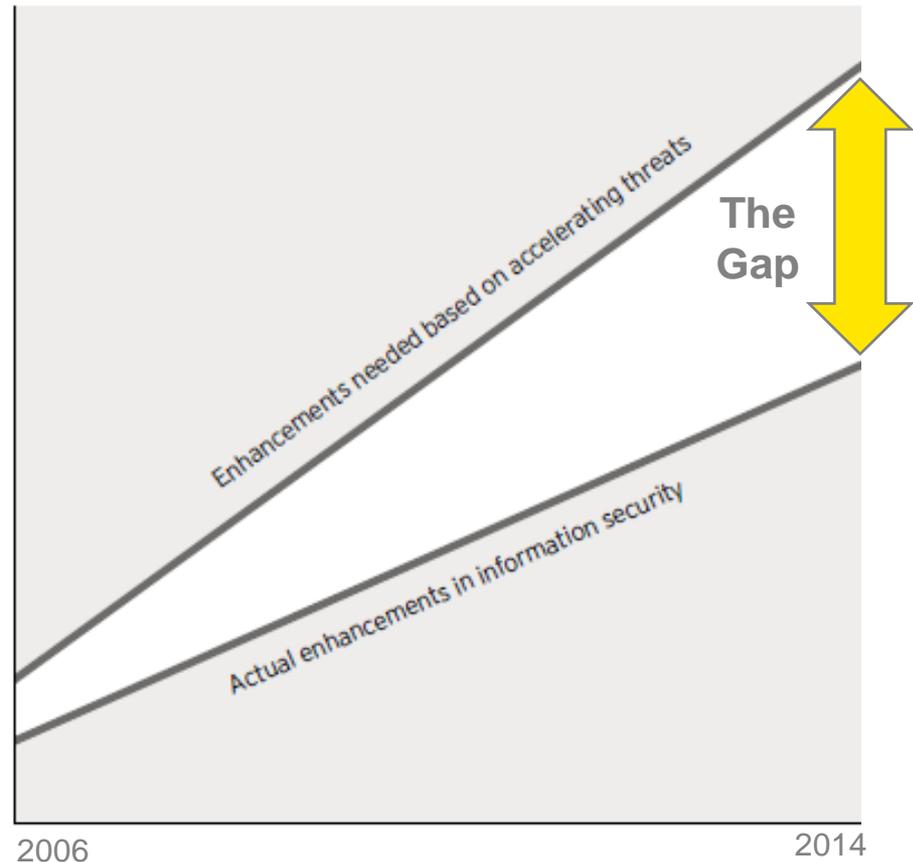
- ▶ **59% of the respondents cite an increase in risk from external threats.**
- ▶ **31% report an increase in the number of security incidents experienced year on year.**
- ▶ **68% of respondents say information security partially meets the needs of the organization.**
- ▶ **50% of respondents cite a lack of skilled resources as a barrier to protecting data.**

Information security is the #1 priority for 2014
National Association of State Chief Information Officers (NASCIO)

Government Employees Cause Nearly 60 Percent of Public Sector Cyber Incidents
NextGov.com (04/22/14)

Many organizations are still fighting to close the gap

- ▶ Organizations have made significant moves to respond to information security threats by addressing vulnerabilities with increased resources, training, governance and integration.
- ▶ However, the number and sophistication of threats has also increased, and is challenging Information Security functions to keep up.
- ▶ As a result, the gap between what Information Security functions *are* doing and *should* be doing has widened.



Cybersecurity from a business and organization leadership perspective



Changing the way organizations think about information security

- ▶ With so much at stake – personal identifiable information, operations and financial data, and organizational reputation – informed **leaders are realizing that it is time for a fundamental rethink** of how information security is understood and positioned within their organization.
 - ▶ **Agency heads need to view the Information Security function in a new light.** Today's information security programs are challenged to effectively deliver value while managing risk.
 - ▶ **Information Security is not a barrier to fast-paced emerging technology** if done right.
 - ▶ **Your Information Security function should be aligned to the needs of citizens** (such as keeping information secure and private), delivering value and enhancing information protection coverage in a cost-effective manner.

Why is leadership in organizations reluctant to tackle cyber security?

- ▶ **A crowded agenda**

Information security is just one of many pressing issues demanding attention, particularly during economic uncertainty

- ▶ **The IT silo**

Digital security has traditionally been viewed as an IT issue - protecting the IT systems that process and store information rather than on the strategic value of the information itself.

- ▶ **“Not our problem”**

Information security is often (wrongly) viewed as a significant problem only in sectors like the military or financial services.

- ▶ **The risks are difficult to gauge**

Cyber threats are hard to predict, making the risks and potential impact difficult to gauge. Senior leaders may feel they lack the expertise necessary to make enterprise-wide decisions or may be wary of being pulled too deeply into technical processes.

- ▶ **Invisible pay-off**

With scarce resources, it's hard to invest money, people and time in the unknown and unpredictable.

Cybersecurity matters to the leadership

What Agency heads are asking

- ▶ Is information security focused on protecting the assets that matter?
- ▶ How do we measure the effectiveness of our information security program?
- ▶ How has the Information Security program kept pace with the evolution of our IT landscape (e.g., cloud, mobile, social, BYOD)?
- ▶ Is the information security organization appropriately organized, trained, equipped, staffed and funded?
- ▶ What are other organizations like us doing?
- ▶ Do we have the ability to detect if we've been breached? Have we been breached? How effectively would we respond to a breach?
- ▶ Do our various control audits address these risks?

Balancing cost, risk and value

- ▶ **Information security programs struggle with the balancing act of reducing costs while identifying gaps in existing security capabilities; and making strategic prioritized investments to address business needs, increase value, and keep the organization secure.**



Are our information security capabilities efficient and effective?

And do we have:

- ▶ Right resources?
- ▶ Right initiatives, processes and technologies?
- ▶ Right investments?

Does our information security program currently:

- ▶ Manage organization security risk?
- ▶ Adequately protect us from new and emerging threats?
- ▶ Identify gaps, and remediate root cause security issues?
- ▶ Proactively respond to changes in the business and regulatory environment?

Will our information security program:

- ▶ Protect brand image and value?
- ▶ Protect assets of most importance to the organization and citizens?
- ▶ Enable new initiatives?

What are organizations doing



Information security requirements in an organization

It is only when cybersecurity is understood within the organization's overall risk management structure that executive leadership can have confidence that their single most important asset – information – is sufficiently protected against today's threats, and tomorrow's. This means understanding and enhancing all your security requirements, which include:

- ▶ Architecture
- ▶ Asset management
- ▶ Awareness
- ▶ Business continuity management
- ▶ Data infrastructure
- ▶ Data protection
- ▶ Governance and organization
- ▶ Host security
- ▶ Identity and access management
- ▶ Incident management
- ▶ Metrics and reporting
- ▶ Network security
- ▶ Operations
- ▶ Policy and standards framework
- ▶ Privacy
- ▶ Security monitoring
- ▶ Software security
- ▶ Strategy
- ▶ Third-party management
- ▶ Threat and vulnerability management

An effective cyber security strategy looks ahead to future opportunities and threats

- ▶ How would your organization's current security framework respond to:
 - ▶ Changes in regulatory risk
 - ▶ Geopolitical shocks
 - ▶ A cyber attack affecting your reputation
 - ▶ Control failures
 - ▶ Information security, resilience and data leakage
 - ▶ Agency consolidation
 - ▶ Using third parties or shared service centres
 - ▶ IP and data security threat (data leakage, loss and rogue employees)

Consider assessing the effectiveness of your information security capabilities

- ▶ **Creating a security program around intelligence on threats and business risks** will support resilience in a constantly shifting landscape of risk.
- ▶ An **assessment** assists with:
 - ▶ Understanding your organization's risk exposure
 - ▶ Assessing the maturity of your current information security program and identifying areas for improvement
 - ▶ Building a prioritized roadmap for project investments and organizational change initiatives
 - ▶ Collecting information to create benchmarks against other organizations
 - ▶ Validating that your security investments have improved your security posture

What organizations should be doing

Identify the real risks:

- ▶ Develop a security strategy focused on business drivers and protecting high-value data
- ▶ Define the organization's overall risk appetite
- ▶ Identify the most important information and applications, where they reside and who has/needs access
- ▶ Assess the threat landscape and develop models highlighting your real exposures

Sustain your security program:

- ▶ Get governance right – make security a board-level priority
- ▶ Allow good security to drive compliance – not vice versa
- ▶ Measure leading indicators to catch problems while they are still small
- ▶ Accept manageable risks that improve performance
- ▶ Know your weaknesses – and address them!

Protect what matters most:

- ▶ Assume breaches will occur – improve processes that complicate, detect and respond
- ▶ Balance the fundamentals with emerging threat and vulnerability management
- ▶ Establish and rationalize access control models for applications and information
- ▶ Protect key identities and roles because they have access to the crown jewels

Embed security in the operation:

- ▶ Make security everyone's responsibility — it's a business problem, not just an IT problem
- ▶ Align all aspects of security (information, privacy, physical and business continuity) with the business
- ▶ Spend wisely in controls and technology – invest more in people and process
- ▶ Selectively consider outsourcing or co-sourcing operational security program areas

Leading practices to combat cyber threats

- ▶ The leading practices that enable improvement:
 - ▶ Commitment from the top
 - ▶ Leadership support
 - ▶ Organizational alignment
 - ▶ Strategy
 - ▶ Investment
 - ▶ People, processes and technology to implement
 - ▶ People
 - ▶ Processes
 - ▶ Technology
 - ▶ Operational enablement
 - ▶ Continuous improvement
 - ▶ Physical security
 - ▶ Analytics and reporting
 - ▶ Environment

Leading practices to combat cyber threats

Commitment from the top

- ▶ **Leadership support** - Organizations need executive support to establish a clear charter for the Information Security function and a long-term strategy for its growth.
 - ▶ **Articulate risk appetite** to provide clear unambiguous direction
 - ▶ **Incentivize timely remediation of security issues**, e.g. via internal audit or information security functions
 - ▶ **Measure information security performance** and the criteria for success
Foster an information security culture throughout all levels of the organization
 - ▶ **Understand how security events can impact the business**, its services and products
 - ▶ **Integrate information security insights directly into management decision making processes**
 - ▶ **Translate information security threats into their impact** (financial, regulatory, reputation, etc.)

Leading practices to combat cyber threats

Organizational alignment

- ▶ **Strategy** - Information Security must develop strong, clearly defined relationships with a wide range of stakeholders across the business, and establish a clearly defined and formalized governance and operating model.
 - ▶ **Align security strategy with overall business strategy**
 - ▶ **Conduct independent third-party assessments** — then get a second, independent opinion
 - ▶ Build an information security organization and operating model that anticipates rather than reacts
- ▶ **Investment** - Organizations need to be willing to invest in cyber security.
 - ▶ **Prioritize security initiatives to drive security investment**
 - ▶ **Categorize expected benefits**, e.g. brand protection, risk reduction, improved compliance and cost reduction
 - ▶ Decrease the spend on maintenance and incidents; increase the spend on improvement and innovation

Leading practices to combat cyber threats

People, processes and technology to implement

- ▶ **People** - Today's Information Security function requires a broad range of capabilities with a diversity of experiences. Technical IT skills alone are no longer enough.
 - ▶ Raise employee awareness of their security responsibilities and appropriate use of organization's assets
 - ▶ Screen and hire the right people with the right skills and competencies, including those in high-risk roles
 - ▶ Make information security part of the performance assessment of employees
 - ▶ Know and control who holds elevated privileges
- ▶ **Processes** - Processes need to be documented and communicated, but Information Security functions also need to develop change management mechanisms to quickly update processes when opportunities for improvement arise.
- ▶ **Technology** - To gain the most value from a technology solution, Information Security functions must supplement their technology deployment efforts with strategic initiatives that address proper governance, process, training and awareness.
 - ▶ Balance the technology choices with the threats and vulnerabilities the technology brings
 - ▶ Ensure information security is an integral part of IT projects
 - ▶ Understand the inventory of technologies you rely on and develop specific standards for them
 - ▶ Develop the capability to monitor technology assets hosting sensitive data and critical business services in real time
 - ▶ Routinely test security at an application level as well as an infrastructure level

Leading practices to combat cyber threats

Operational enablement

- ▶ **Continuous improvement** - Organizations must establish a framework for continuously monitoring performance and improving their information security programs in the areas of people, process and technology.
- ▶ **Physical security** - Organizations should ensure that all their information security technology is physically secure, especially with consideration for access to WiFi. A security operations center (SOC) can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively.
- ▶ **Analytics and reporting** - Signature and rule-based tools are no longer as effective in today's environment. Instead, Information Security functions may wish to consider using behavior-based analytics against environmental baselines.
- ▶ **Environment** - Information Security requires an environment that includes a well-maintained enterprise asset management system (which includes criticality of supported business processes) to manage events associated with business priorities and assess the true risk or impact to the organization.

Questions and thank you



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.

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, 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.

© 2014 Ernst & Young LLP
All Rights Reserved.

www.ey.com/GRCinsights