The Evolving IT Risk Landscape

29 December 2014

IT risk megatrends

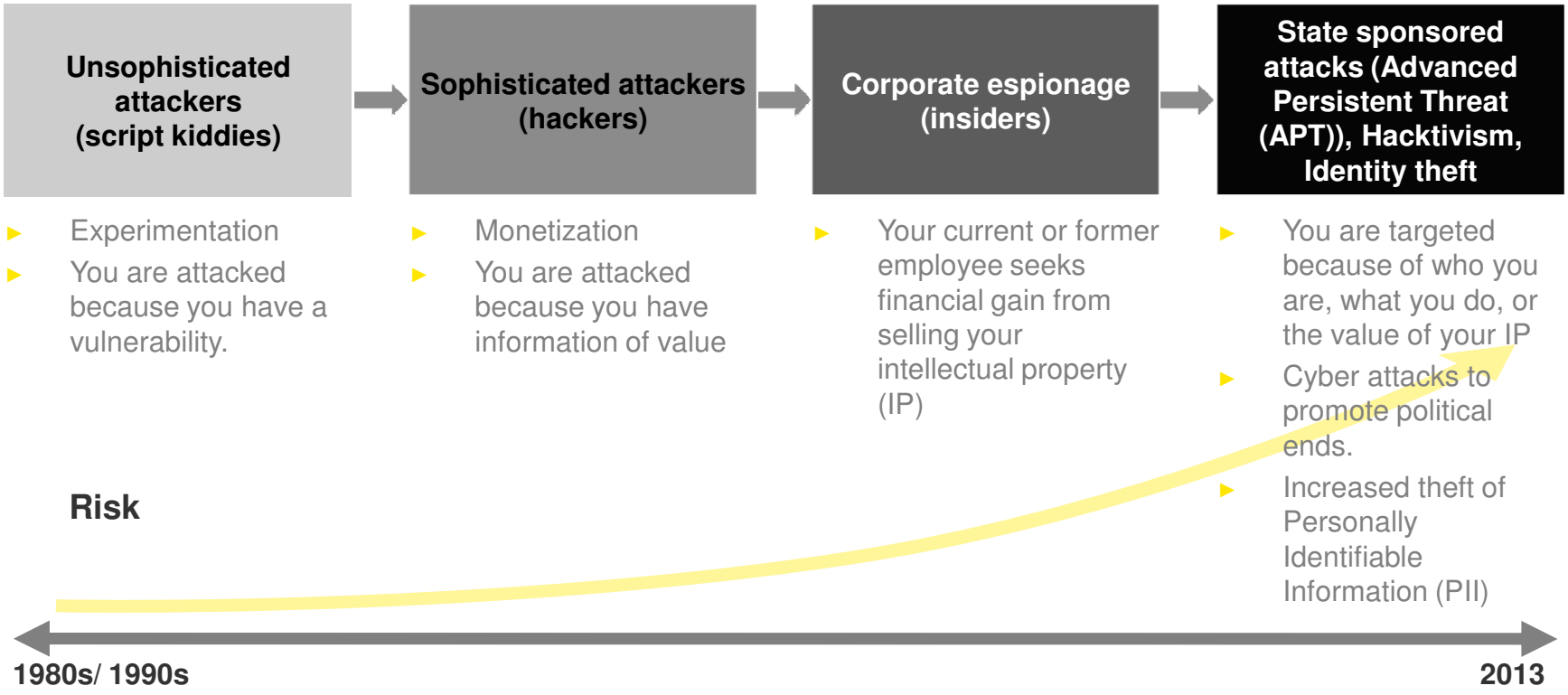
Enhanced persistence of cybercrime	► Spread of malicious code in company systems causing system outages ► The risk of theft of personal, financial, and health information ► Financial loss due to unauthorized wire transfers
Increased exposure to internal threats	► Assigning access rights that are beyond what is required for the role by employees or contractors ► Failure to remove access rights for employees or contractors on leaving the organization
Emerging consumerization (Mobile computing/ social media)	► Increased vulnerability due to anytime, anywhere accessibility ► Risk of unintended sharing, amplification of casual remarks, and disclosure of personal and company data.

IT risk megatrends (contd.)

The rise of cloud computing	► Lack of governance and oversight over IT infrastructure, applications and databases ► Vendor lock-in, Privacy and security ► Availability of IT to be impacted by the use of the cloud
The increased importance of business continuity	► Failure of the business continuity and disaster recovery plans causing financial or reputational loss
The accelerating change agenda	► Failure to deliver IT projects and programs within budget, timing, quality and scope causing value leakage

Security threats have evolved

- Attackers today are patient, persistent, and sophisticated, and attack not only technology, but increasingly, people and processes. The challenges faced today have altered expectations, strained resources, and caused a paradigm shift in information security processes.
- Consequently, we need to alter their mindset on how we think about information security threats, risks, and capabilities.



10 IT Risks to be considered for IT audits

Information security

IT internal audit plays a key role in evaluating the organizations security posture and strategy.

Key questions to evaluate during audit	
Information security program assessment	▸ How comprehensive of an information security program exists? ▸ Is information security embedded within the organization, or is it an "IT only" responsibility? ▸ How well does the organization self-assess threats and mitigate the threats?
Threat and vulnerability management program assessment	▸ How comprehensive of a threat and vulnerability management program exists? ▸ Are the components of TVM integrated with one another, as well as with other security and IT functions? ▸ Do processes exist to address that identified issues are appropriately addressed and remediation is effective?
Vulnerability assessment	▸ What mechanisms are in place to complicate attacks the organization is concerned about? ▸ What vulnerabilities exist and are exploits of these vulnerabilities detected? ▸ What is the organizations response time when intrusion is detected?

Business continuity

A focused business continuity program helps identify the key points of failure and build in redundancy to ensure continuity of operations during a disaster

Key questions to evaluate during audit	
Business continuity program integration and governance audit	▸ Does a holistic business continuity plan exist for the organization? ▸ How does the plan compare to leading practice? ▸ Is the plan tested?
Disaster recovery audit	▸ Are disaster recovery plans aligned with broader business continuity plans? ▸ Do testing efforts provide confidence systems that can be effectively recovered? ▸ Are all critical systems included? Are critical systems defined?
Crisis management audit	▸ Are crisis management plans aligned with broader business continuity plans? ▸ Are plans comprehensive and do they involve the right corporate functions? ▸ Are plans well communicated?

Mobile technology

It is important to identify the risks associated with the use of mobile devices and implement adequate safeguards to secure the information.

Key questions to evaluate during audit	
Mobile device configuration review	▸ How has the organization implemented “bring your own device” (BYOD)? ▸ Are the right policies/mobile strategies in place? ▸ Are mobile devices managed in a consistent manner? ▸ Are configuration settings secure and enforced through policy? ▸ How do we manage lost and stolen devices? ▸ What vulnerabilities exist, and how do we manage them?
Mobile application black box assessment	▸ What vulnerabilities can be successfully exploited? ▸ How do we respond when exploited, and do we know an intrusion has occurred?
Mobile application gray box assessment	▸ How sound is the code associated with the mobile applications used within the organization? ▸ What vulnerabilities can be exploited within the code?

Cloud

A lot of critical data may be stored within the cloud space, hence it is imperative to assess the security and complement with appropriate safeguarding of the data.

Key questions to evaluate during audit	
Cloud strategy and governance audit	▸ Is there a strategy around the use of cloud providers? ▸ Are there supporting policies to follow when using a cloud provider? Are policies integrated with legal, procurement and IT policies?
Cloud security and privacy review	▸ Has a business impact assessment been conducted for the services moving to the cloud? ▸ Does your organization have secure authentication protocols for users working in the cloud? ▸ Have the right safeguards been contractually established with the provider?
Cloud provider service review	▸ What SLAs are in place for uptime, issue management and overall service? ▸ Has the cloud provider been meeting or exceeding the SLAs? What issues have there been? ▸ Does the organization have an inventory of uses of external cloud service providers, both sponsored within IT or direct by the business units?

IT risk management

IT risk management aims at a holistic IT risk program and provide updates to the leadership.

Key questions to evaluate during audit	
IT risk management strategy assessment	► How well does IT identify risks? What is done once a risk is identified? ► Does your IT risk program cover all of IT including shadow IT? ► How are IT risks identified, remediated or accepted?
IT governance audit	► Do formalized processes to govern IT exist? ► What can be done to increase business confidence in IT governance? ► Are your IT governance processes and requirements applicable across all of IT? ► Are there formal charters, mandates and responsibilities documented and followed by key steering committees?
IT risk assessment	► Is there a comprehensive risk assessment performed to identify all IT risks? ► Is there an opportunity to coordinate the IT internal audit risk assessment with IT's own risk assessment?
Technology enablement/GRC package selection	► How can GRC software be effectively used within the organization? ► What is the level of risk reporting provided to stakeholders to support IT risk decisions?

EY

Program risk

With increased spend on large enterprise IT initiatives it becomes important to ensure that the program interdependencies and delivery is tracked.

Key questions to evaluate during audit	
Project management methodology audit	► Are the right processes and controls in place to provide that projects are delivered on time, on budget and with the right resources? ► Are controls in place to measure achieved benefits against intended benefits after project completion?
Project and program execution audit	► Is project/program management methodology being followed correctly? ► What is done when projects are under-performing? ► How is project risk assessed and managed?
Portfolio risk review	► Do the right governance processes exist to provide that projects/programs align to company strategy? ► How is the portfolio managed as corporate objectives change?

IT asset management

Efficient IT asset tracking is required to manage contract and licensing risks and associated penalties.

Key questions to evaluate during audit	
IT and software asset management process and control audit	▸ Do we have a comprehensive approach to IT asset and software management? ▸ How well do we manage software license costs? ▸ Is there an IT and software asset management technology solution in place to support these processes? If not, should there be?
Software license review	▸ Are there opportunities to renegotiate software licensing agreements based on the way we actually utilize software versus the way original contracts were negotiated? ▸ Are we violating any existing contractual agreements?
IT contract management assessment	▸ Are IT asset and software contracts planned, executed, managed and monitored effectively? ▸ Are there “shadow IT” contractual agreements executed in other parts of the organization?

Social media risk management

Lack of employee guidelines around social media may lead to them leaking sensitive information on networking sites.

Key questions to evaluate during audit	
Social media risk assessment	▸ Does the organization understand what risks exist related to social media? ▸ How well are the identified risks managed?
Social media governance audit	▸ Does a governance process exist for social media within the organization? ▸ How well are policies related to social media known amongst employees?
Social media activities audit	▸ Are social media activities aligned to policy? ▸ What corrective actions need to be put in place given activity? ▸ How does existing activity affect brand and reputation?

Segregation of duties

SOD is an increasing challenge with the growing complexity of IT applications. Effectively assigning access and ensuring a conflict free environment is a challenge

Key questions to evaluate during audit	
Systematic segregation of duties review audit	▸ How does IT work with the business to identify cross-application segregation of duties issues? ▸ Does business personnel understand ERP roles well enough to perform user access reviews? ▸ While compensating controls identified for SoD conflicts may detect financial misstatement, would they truly detect fraud?
Role design audit	▸ Does the organization design roles in a way that creates inherent SoD issues? ▸ Do business users understand the access being assigned to roles they are assigned ownership of?
Segregation of duties remediation audit	▸ Does the organization take appropriate action when SoD conflicts are identified? ▸ Have we proactively addressed SoD issues to prevent year-end audit issues?
IAM/GRC technology assessment	▸ Is IAM or GRC software currently used effectively to manage SoD risk? ▸ What software could be utilized to improve our level of SoD control, and what are our business requirements?

Data loss prevention/ privacy

Losing sensitive data can be a nightmare for companies. Implementing tools to detect and flag loss / leakage of data sensitive to an organization is of importance.

Key questions to evaluate during audit	
Data governance and classification audit	▸ What sensitive data do we hold — what is our most important data? ▸ Where does our sensitive data reside, both internally and with third parties? ▸ Where is our data going?
DLP control review	▸ What controls do we have in place to protect data? ▸ How well do these controls operate? ▸ Where do our vulnerabilities exist, and what must be done to manage these gaps?
Privacy regulation audit	▸ How well do we understand the privacy regulations that affect our global business? For example, HIPAA is potentially a risk to all organizations, not just health care providers or payers. ▸ Do we update and communicate policies in a timely manner? ▸ Do users follow control procedures to address regulations?


Thank you
Nitin Mehta
Director, Advisory Services
Ernst & Young LLP
EY
Building a better working world
100+
YEARS OF EXCELLENCE IN PROFESSIONAL SERVICES