Cyber

Paul Torres – Director

KPMG Cyber Practice

October 9, 2018

FOR TRAINING PURPOSE ONLY

Agenda

- Cyber fundamentals
- Typical cybersecurity assessment
- Cyber Trends
- Internal audit role in cyber
- Wrap up

KPMG

Cyber fundamentals

Cyber fundamentals

Definition

“The protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.”

Information Security vs. Cybersecurity

Information security

Focus: Protection of information, regardless of format, including:

— Paper documents

— Digital and intellectual property

— Verbal or visual communications

Cybersecurity

Focus: Protection of digital assets, including:

— Network hardware

— Software

— Information processed and stored in isolated or network systems

ISACA®
Trust in, and value from, information systems

Cyber fundamentals

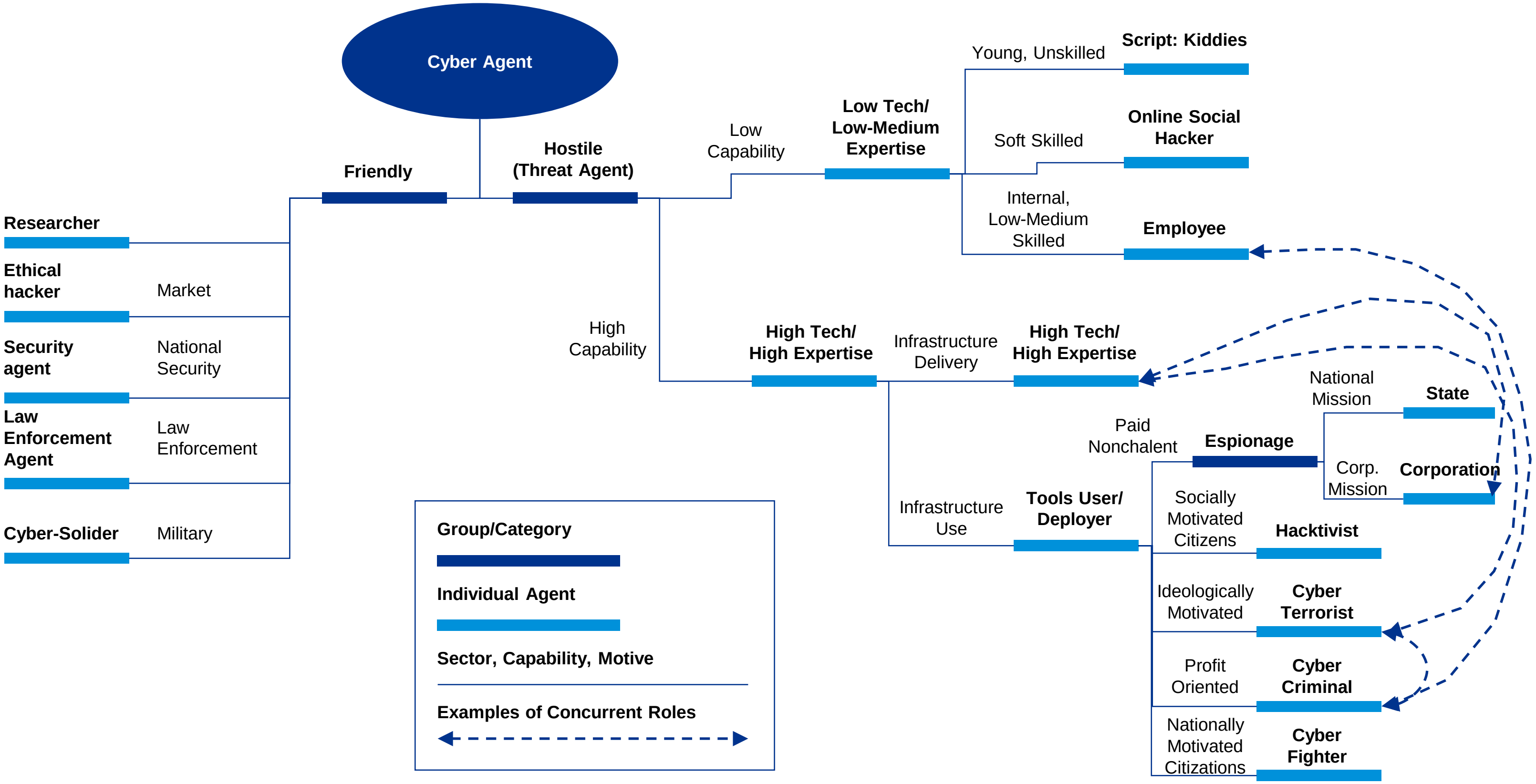
The History of

The Nist Cybersecurity framework

EO 13535 **2013**	Pre. Obama signs Order to improve security for critical Infrastructure, increase communication of threats, & involve private sector
NIST VERSION 1 **2014**	Department of Homeland Security (DHS) gets input from private sector subject-matter experts
PUBLIC LAW 113-385 **2014**	Cybersecurity Enhancement Act reinforces future framework & supports voluntary, industry-led cybersecurity standards
2015+	NIST recommends non-critical infrastructure organizations also adopt the Framework

Cyber fundamentals

Common threat agents



Cyber Agent

Friendly

Researcher

Ethical hacker — Market

Security agent — National Security

Law Enforcement Agent — Law Enforcement

Cyber-Solider — Military

Hostile (Threat Agent)

Low Capability — Low Tech/ Low-Medium Expertise

- Young, Unskilled — Script: Kiddies
- Soft Skilled — Online Social Hacker
- Internal, Low-Medium Skilled — Employee

High Capability — High Tech/ High Expertise

- Infrastructure Delivery — High Tech/ High Expertise
- Infrastructure Use — Tools User/ Deployer
  - Paid Nonchalent — Espionage
    - National Mission — State
    - Corp. Mission — Corporation
  - Socially Motivated Citizens — Hacktivist
  - Ideologically Motivated — Cyber Terrorist
  - Profit Oriented — Cyber Criminal
  - Nationally Motivated Citizations — Cyber Fighter

Group/Category

Individual Agent

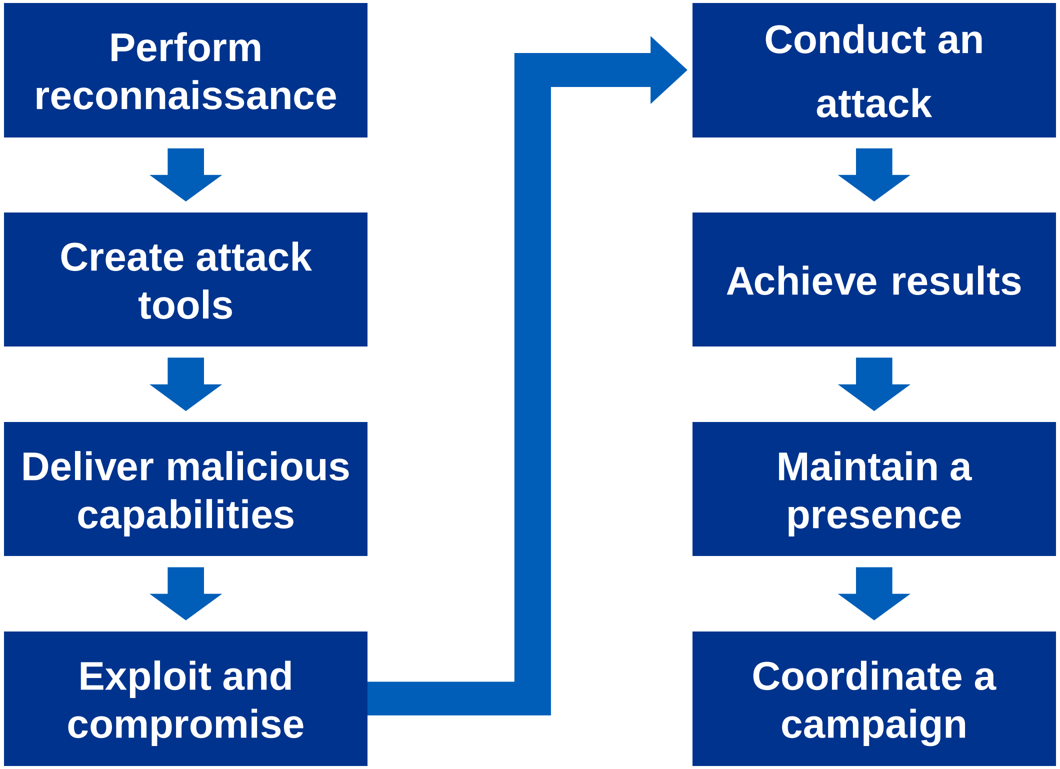
Sector, Capability, Motive

Examples of Concurrent Roles

Source: Marinos, Louis, A. Belmonte, E. Rekleitis, “ENISA Threat Landscape 2015,” ENISA, January 2016, Greece

Cyber fundamentals

Threat process



Perform reconnaissance

Create attack tools

Deliver malicious capabilities

Exploit and compromise

Conduct an attack

Achieve results

Maintain a presence

Coordinate a campaign

Cyber fundamentals

Malware and attack types

Virus	Keylogger	DoS
Worm	Rootkit	Man-in-the-middle
Trojan horse	APT	Social engineering
Botnet	Backdoor	Phishing
Spyware	Brute force	Spoofing
Adware	Buffer overflow	SQL injection
Ransomware	XSS	Zero-day exploit

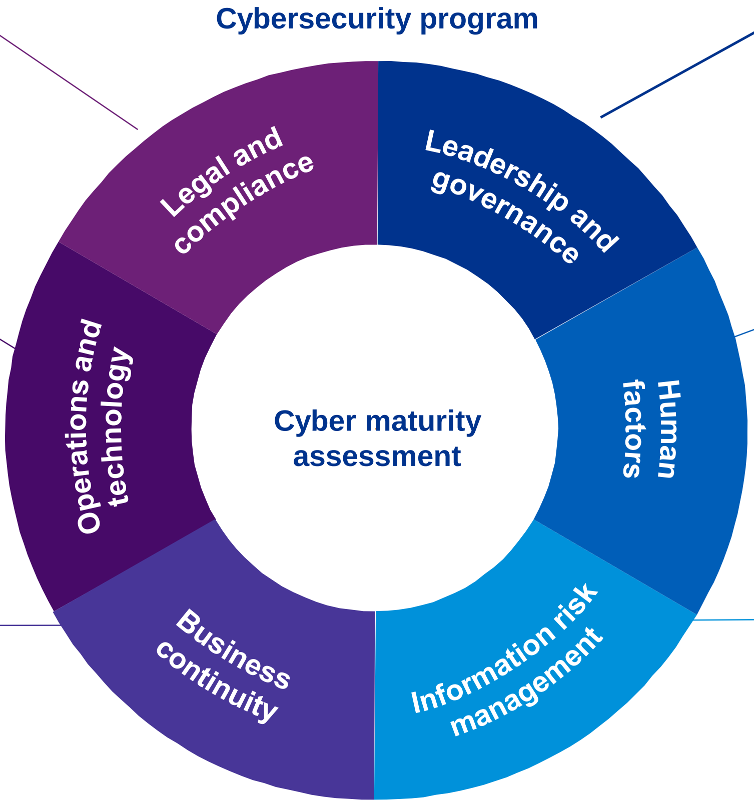
Cyber fundamentals

Function unique identifier	Function	Category unique identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

KPMG

Typical cybersecurity assessment


Cybersecurity program
Legal and compliance
Leadership and governance
Human factors
Information risk management
Business continuity
Operations and technology
Cyber maturity assessment

Legal and compliance

Regulatory and international certification standards as relevant

Operations and technology

The level of control measures implemented to address identified risks and minimize the impact of compromise

Business continuity and crisis management

Preparations for a security event and ability to prevent or minimize the impact through successful crisis and stakeholder Management

Leadership and governance

Board demonstrating due diligence, ownership and effective management of risk

Human factors

The level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge

Information risk management

The approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners

Typical cybersecurity assessment

Three focus areas when assessing cybersecurity program

People

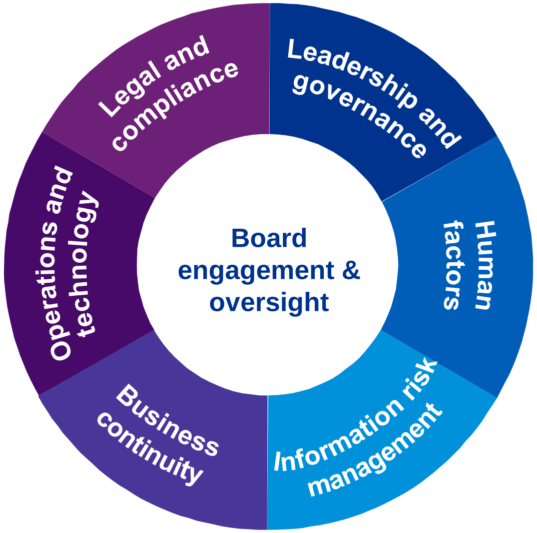
- Leadership & Governance
- Human Factors

Process

- Legal & Compliance
- Business Continuity

Technology

- Information Risk Management
- Operational and Technology

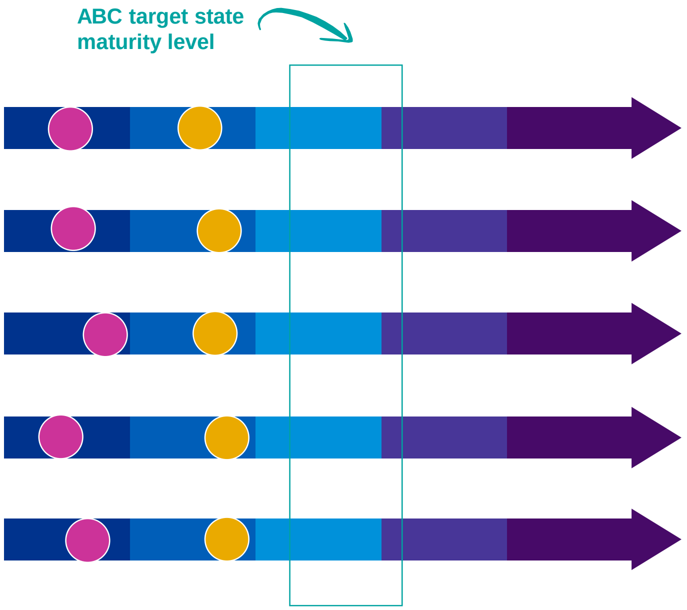

Board engagement & oversight
Leadership and governance
Human factors
Information risk management
Business continuity
Operations and technology
Legal and compliance

Typical cybersecurity assessment

2018 CMA Results – As noted in the Executive Summary, ABC' cybersecurity program has established fundamental security processes and tools that would be characterized as having a 2-REPEATABLE security posture. ABC should continue to mature the cybersecurity program by implementing the (14) recommendations we noted and manage the overall program towards the defined 3-DEFINED future state. The next pages will discussed in details the (14) recommendations that will help ABC move its cybersecurity program towards 3-DEFINED future state.

2016 vs 2018 Comparison – Below also provides an overview comparison between 2016 vs. 2018 results of the state of each of the cybersecurity domain.

Dimension | Maturity level | Scores



Dimension	Current state	Proposed target state	Proposed Timeline
Leadership and Governance	2	3	6 – 12 months
Security and Configuration Management	2	3	6 – 12 months
Incident Response	2	3	6 – 12 months
Security Architecture	2	3	6 – 12 months
Threats and Vulnerability Management	2	3	6 – 12 months

Initial – 1
Ad hoc, unpredictable, poorly controlled, reactive

Repeatable – 2
Basic processes management, repeatable tasks

Defined – 3
Defined and documented processes, proactive

Managed – 4
Processes integrated, measured, and controlled

Optimized – 5
Continual improvement, organizational alignment

● 2016 state

● Current state

□ Proposed Target State

Typical cybersecurity assessment

Example external and internal vulnerability scanning approach:

	Intelligence Gathering	Reconnaissance	Enumeration	Validation	Exploitation	Lateral Movement	Exfiltration	End of attack	
Actions	Open source and public information gathering of the system to be tested to inform test and attack planning and threat modeling	Perform initial attack surface identification of in-scope system to identify features, functions and possible vulnerabilities	Perform automated vulnerability scanning to rapidly identify potential system vulnerability	Perform of previously identified vulnerabilities removing false positives/ negatives	Leveraging previously identified findings and attempting to exploit these findings to gain access to gain access to additional assets or information or elevate access	Upon completion of all enumeration, validation and exploitation testing, perform re-assessment to determine possible new testing scenarios or attack options	Elevate user system access or attempt to collect additional system data or remove system assets	Attacker terminates defined attack scenario	
Observables	No system contact	Web proxy logs	Reverse proxy logs O365 mailbox audit logs	Local event logs Web proxy logs O365 mailbox audit logs	Local memory forensics Local disks forensics Splunk/ SIEM Alerting	Local disks forensics Web proxy logs	Local disks forensics DLP logs/alerts New flow logs		

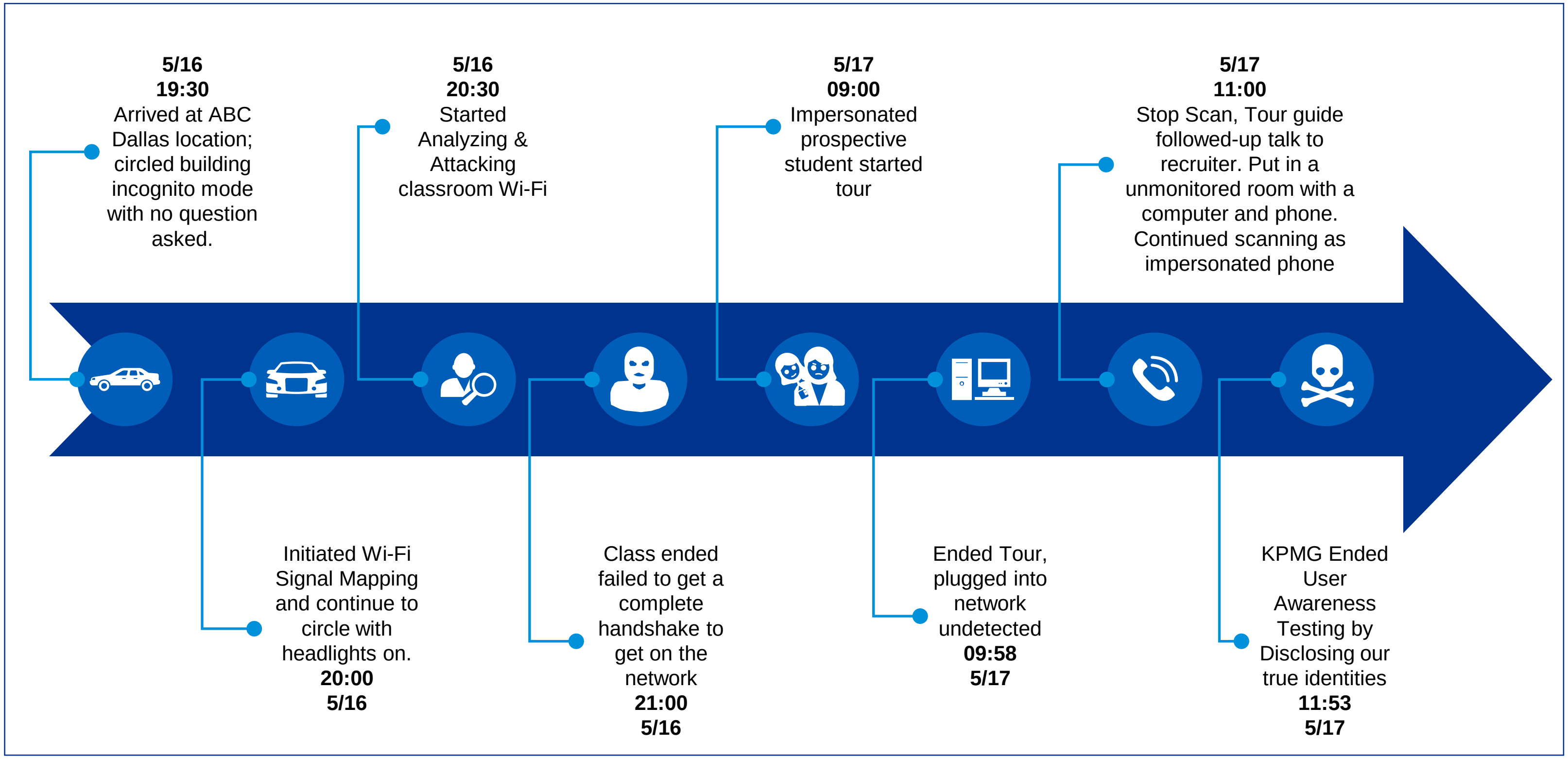
Typical cybersecurity assessment

Example social engineering approach:

— Email phishing – Our approach will be more of a training/educational exercise.

— Pre-texting – Test scenario to be executed and target names and corresponding contact information.

— Wireless – Attempt to penetrate wireless LAN infrastructure & surrounding network system and identify wireless points of presence (blind-find and known technique).



5/16
19:30
Arrived at ABC Dallas location; circled building incognito mode with no question asked.

Initiated Wi-Fi Signal Mapping and continue to circle with headlights on.
20:00
5/16

5/16
20:30
Started Analyzing & Attacking classroom Wi-Fi

Class ended failed to get a complete handshake to get on the network
21:00
5/16

5/17
09:00
Impersonated prospective student started tour

Ended Tour, plugged into network undetected
09:58
5/17

5/17
11:00
Stop Scan, Tour guide followed-up talk to recruiter. Put in a unmonitored room with a computer and phone. Continued scanning as impersonated phone

KPMG Ended User Awareness Testing by Disclosing our true identities
11:53
5/17

Typical cybersecurity assessment

This following graphic illustrates typical approach for performing Cybersecurity Assessment.

Assessment areas	Assessment domains		
Cyber Maturity Assessment	Security Configuration Management	Security Architecture	Threat & Vulnerability Management
	Incident Response	BCP/DRP	Logging & Monitoring
External & Internal Vulnerability	Perimeter & Internal Network Vulnerability Assessment	Web Application Security Assessment	

Additional cyber areas to consider

Inside Threat	Identity Management	Data Loss Prevention	User Awareness	End Point Security
Customer Privacy	Access Control	Cloud Security	3rd Party Risk	Security Monitoring

Most common root cause

Configuration Management

Considerations

Configuration management focuses on maintaining the security of IT resources

- Verification of the impact on related items
- Assessment of risk related to a proposed change
- Ability to inspect different lines of defense for potential weaknesses
- Tracking of configuration items against approved secure baselines
- Insights into investigations after a security breached or operations disruption
- Version control and production authorization of hardware and software components

Most common root cause

Patch Management

Considerations

- Software patches are solutions to programming errors, some of which may introduce security vulnerabilities
- Software vendors release regular software updates and patches as vulnerabilities are identified and repaired
- Processes to identify patches that are relevant to IT infrastructure
- Patches should be tested to ensure it does not negatively impact operations
- Patching should be scheduled and the update installed where appropriate

Most common root cause

List of Internal Findings			
Index	Vulnerability	Risk	Root Cause
IT-1	LLMNR and NBT-NS Poisoning	Critical	Configuration Management
IT-2	Colubris Networks Wireless Access Point Default Credentials	Critical	Configuration Management
IT-3	Emerson Network Power Default Credentials	Critical	Configuration Management
IT-4	Nutanix Controller Default Credentials	Critical	Configuration Management
IT-5	Microsoft Windows Unsupported Operating System	Critical	Lifecycle Management
IT-6	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution	Critical	Patch Management
IT-7	Microsoft Windows SMBv1 Multiple Vulnerabilities	Critical	Configuration Management
IT-8	Microsoft IIS 6.0 Unsupported Version Detection	Critical	Lifecycle Management
IT-9	Symantec pcAnywhere Unsupported	Critical	Lifecycle Management
IT-10	MS17-010: Security Update for Microsoft Windows SMB Server	Critical	Patch Management
IT-11	HP Data Protector 8.x Arbitrary Command Execution	Critical	Patch Management
IT-12	McAfee Agent Unsupported Version Detection	Critical	Lifecycle Management
IT-13	VxWorks WDB Debug Service Detection	Critical	Configuration Management
IT-14	Unprotected Telnet Service	Critical	Configuration Management
IT-15	Ipswitch WhatsUp Gold < 16.4 Multiple Vulnerabilities	High	Patch Management
IT-16	FTP Privileged Port Bounce Scan	High	Configuration Management
IT-17	SSL Version 2 and 3 Protocol Detection	High	Configuration Management
IT-18	Oracle TNS Listener Remote Poisoning	High	Patch Management
IT-19	IPMI v2.0 Password Hash Disclosure	High	Configuration Management
IT-20	SNMP Agent Default Community Name (public)	High	Configuration Management

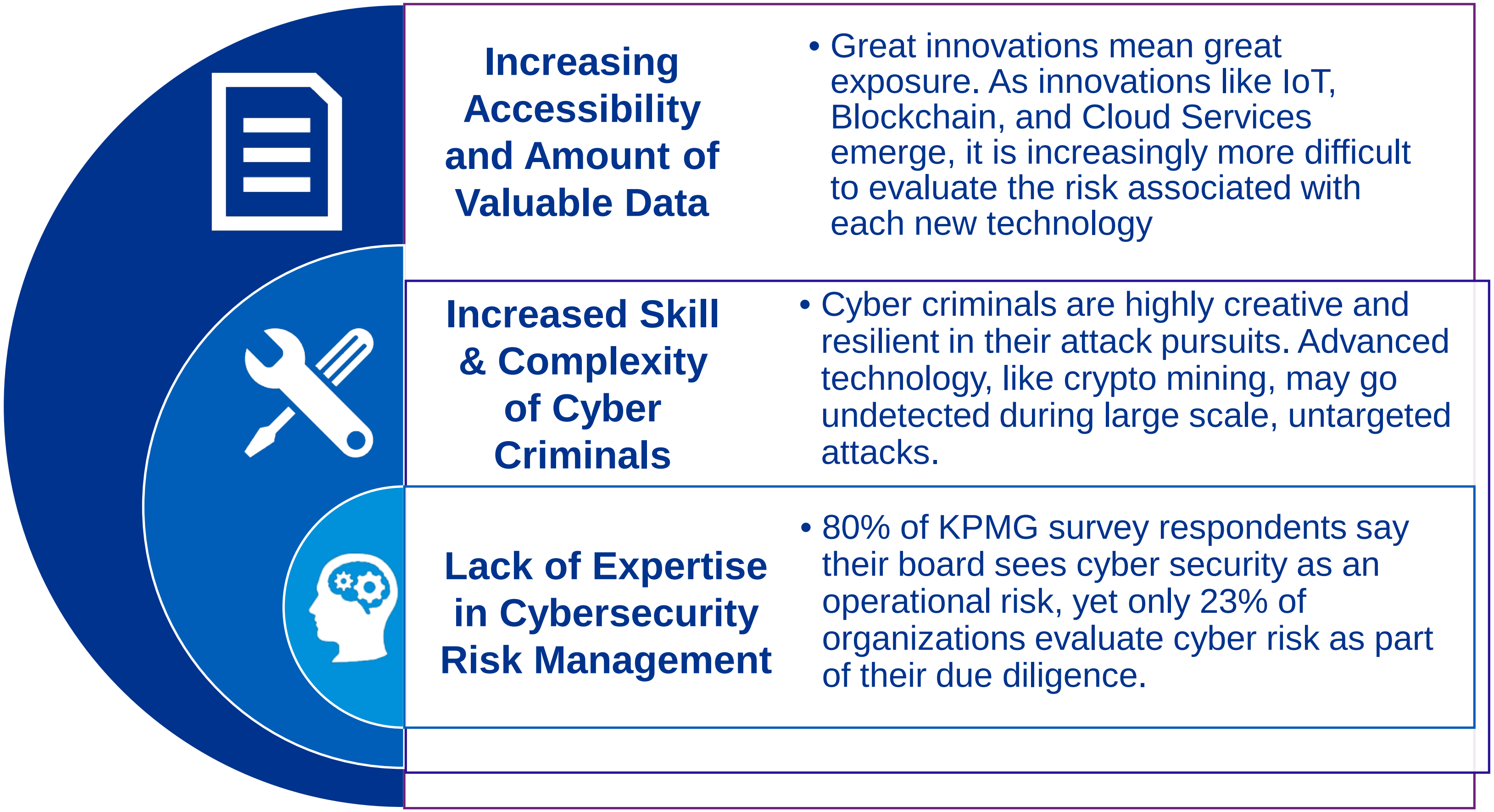
Cyber Trends

Most Recent Cyber Attacks

Company	Case	Result
City of Atlanta 	**Ransomware** March 2018 - SamSam, a custom infection used for targeted attacks, locked City of Atlanta's files via encryption, limiting access to crucial data until a ransom was paid to the attackers.	A ransom of $51,000 was paid to the attackers. The citizens of Atlanta lost a great deal of trust, as the malware impacted what customers use to pay bills and access court-related information.
Tesla	**Insider Attack** June 2018 - A Tesla Employee employed damaging code changes to its manufacturing OS, and sent sensitive Tesla data to unknown 3rd parties.	Investigators suggest that the data that was compromised was sold to competitors, causing Tesla a loss of competitive edge. Full impact of the attacker's actions are still unknown.
Uber	**3rd Party Cloud** November 2017 - An attack on Uber's third-party Cloud infrastructure system allowed the download the information of 57 million users.	Uber paid the attackers a ransom of $100,000 before alerting authorities and users. Uber claims that it obtained assurances that stolen data was destroyed, however the loss of trust from consumers is inevitable.
Equifax ✱✱✱_	**Application Vulnerability Breach** May 2017 - Sensitive customer data, including personal information, and credit card numbers, was stolen from Equifax customers.	Personal information was compromised from over 143 million Americans, and credit card information was stolen from over 209 million Americans. Equifax faced serious loss of trust from its customers as well as loss of business to its competitors.

Influences on Financial Security Ecosystem

Based on the 60 corperate respondents to KPMG’s internal 2018 Cybersecurity survey, the influence on today’s Cyber landscape can be summarized by 3 key elements:



Increasing Accessibility and Amount of Valuable Data

- Great innovations mean great exposure. As innovations like IoT, Blockchain, and Cloud Services emerge, it is increasingly more difficult to evaluate the risk associated with each new technology

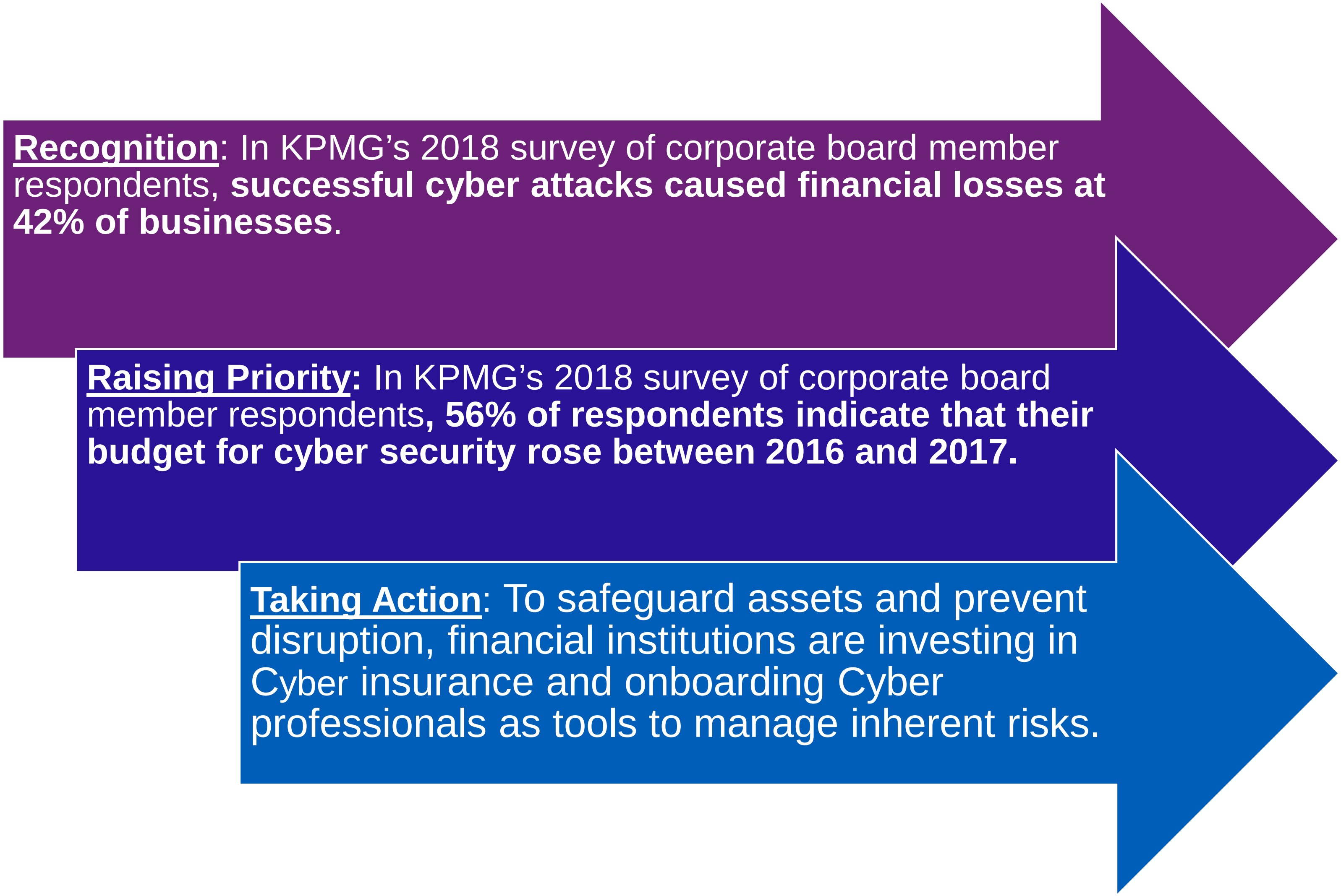
Increased Skill & Complexity of Cyber Criminals

- Cyber criminals are highly creative and resilient in their attack pursuits. Advanced technology, like crypto mining, may go undetected during large scale, untargeted attacks.

Lack of Expertise in Cybersecurity Risk Management

- 80% of KPMG survey respondents say their board sees cyber security as an operational risk, yet only 23% of organizations evaluate cyber risk as part of their due diligence.

Taking Action – Where is your organization at?



Recognition: In KPMG’s 2018 survey of corporate board member respondents, **successful cyber attacks caused financial losses at 42% of businesses**.

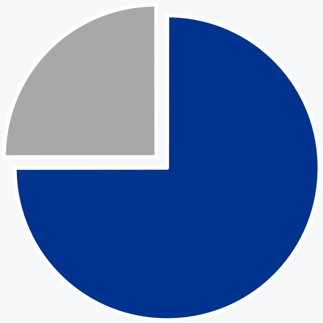
Raising Priority: In KPMG’s 2018 survey of corporate board member respondents**, 56% of respondents indicate that their budget for cyber security rose between 2016 and 2017.**

Taking Action: To safeguard assets and prevent disruption, financial institutions are investing in Cyber insurance and onboarding Cyber professionals as tools to manage inherent risks.

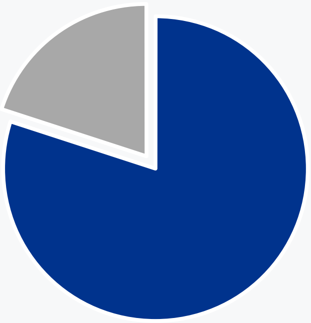
Key Findings

- In 2018, an internal survey was conducted by KPMG inquiring of board members from 60 different companies about their experiences and opinions regarding cybersecurity concerns.

- Financial Services firms are a large **target** within a rapidly changing environment.
- Cyber risk mitigation has received a great deal of attention, but not enough **action**.



75% of successful cyber attacks in financial services resulted in financial losses, compared to 25% in non-financial services.



80% of boards consider cyber security to be an operational risk. But only 36% address the topic in their annual report.

Cyber trend

Cyber readiness

According to organizations, following are the top five cyber areas where investments are provided pertaining to cybersecurity:

75%
Cyber awareness measures

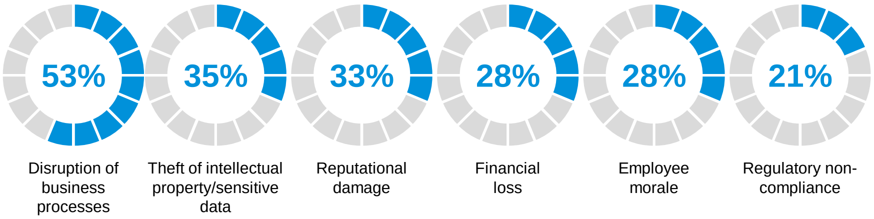
73%
Cyber risk assessment

65%
Incident response planning

65%
Technology investments

45%
Development of cybersecurity framework

Cyber attack targets and impact



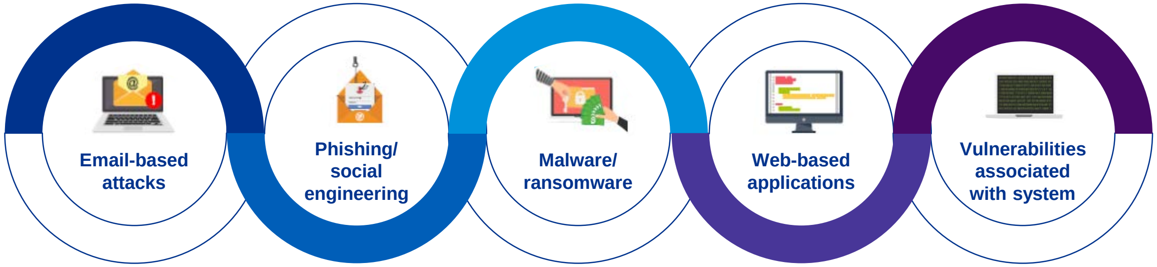
Cyber Trend

Targets for cyber attacks

There are multiple systems and technologies that are being targeted by attackers, using multiple attack measures. There is constant movement towards

Targeted attacks, which is increasing the likelihood of attacks to take place.

Based on the study, top five attacks faced are:



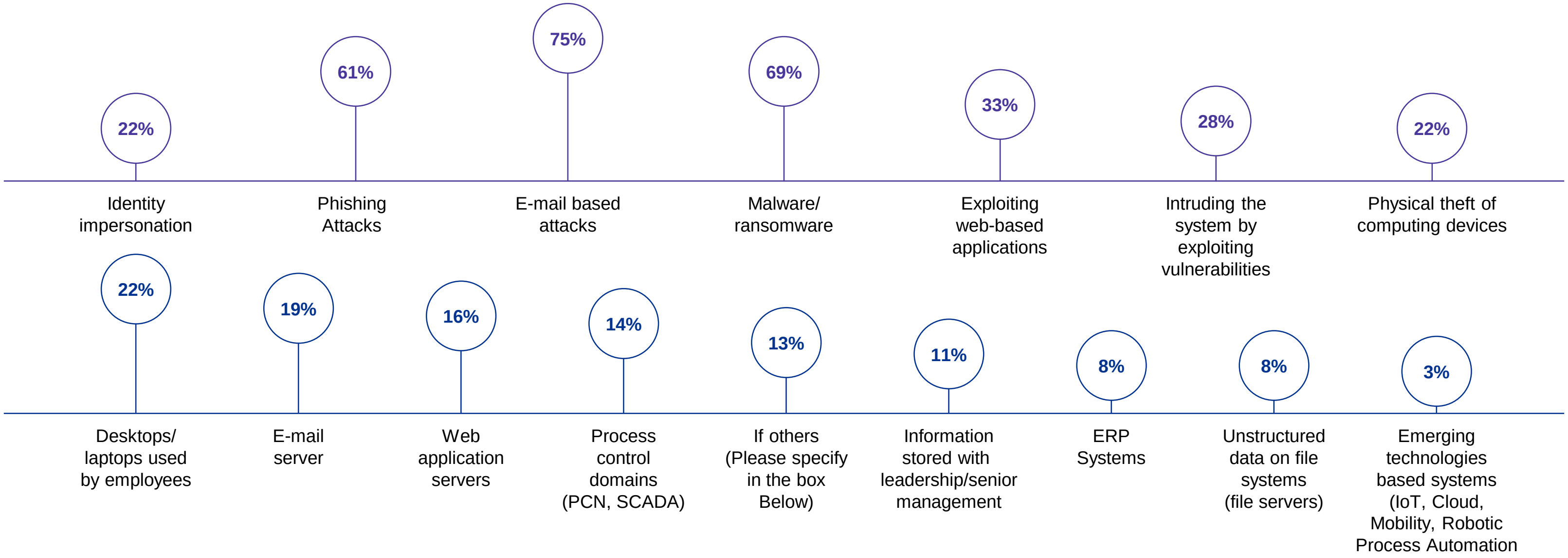
Email-based attacks

Phishing/ social engineering

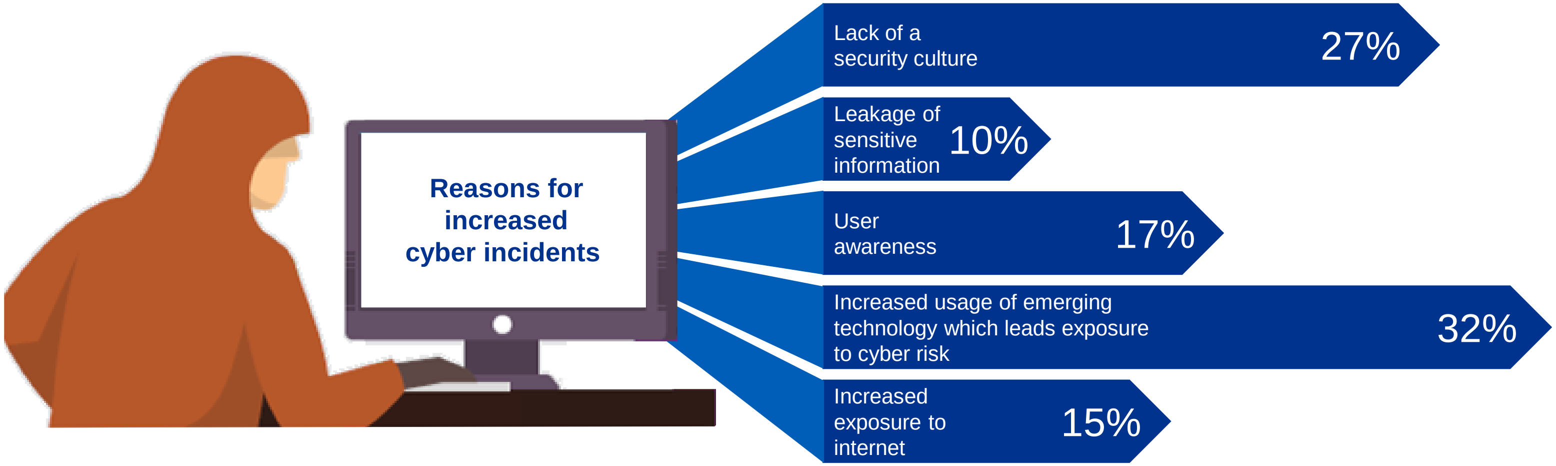
Malware/ ransomware

Web-based applications

Vulnerabilities associated with system



Cyber Trend



Reasons for increased cyber incidents

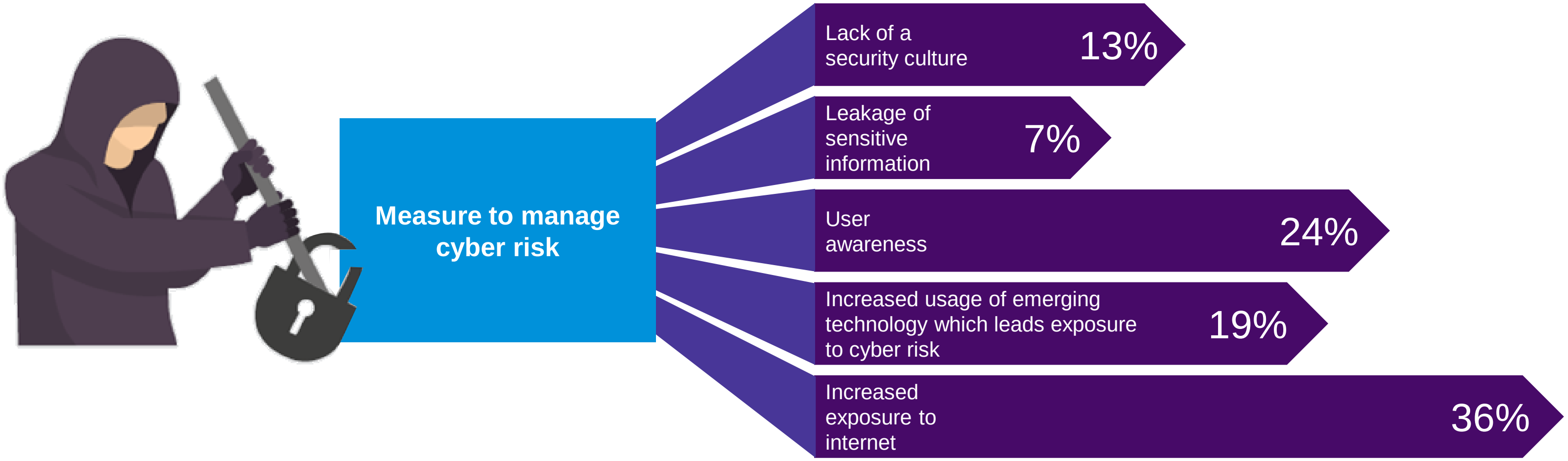
Lack of a security culture 27%

Leakage of sensitive information 10%

User awareness 17%

Increased usage of emerging technology which leads exposure to cyber risk 32%

Increased exposure to internet 15%



Measure to manage cyber risk

Lack of a security culture 13%

Leakage of sensitive information 7%

User awareness 24%

Increased usage of emerging technology which leads exposure to cyber risk 19%

Increased exposure to internet 36%

The 4 “Golden Rules” of cyber security

Get the basics right.

Over 75 percent of attacks exploit failures to put in place basic controls.

Look after your crown jewels.

You have to prioritize where you spend your money to defend yourself, so build a fortress around your most critical assets.

Do your homework on your enemies.

Invest in understanding who might attack you, why and how so that you can anticipate the most likely scenarios and you defend those assets that are most likely to get attacked.

Treat cyber risk as an opportunity to look closely at your business.

Security and resilience can affect nearly every part of an organization. Strategies to protect IT security and business resiliency should align with an organization’s broader goals — from protecting intellectual property to maximizing productivity to finding new ways to delight customers.

Internal Audit Role in Cyber

Cyber trend

KPMG

Strategies for the third line of defense

Internal audit strategies are critical as technologies evolve and business environments change

Cyber trend

Example focus areas for internal audit:

- Perform a top-down risk assessment around the company's cybersecurity process using industry standards as a guide, and providing recommendations for process improvements
- Assess personal data transfer channels and lineage to confirm alignment with stakeholder documentation and understanding
- Evaluate existing processes and controls, such as data retention policies or identity access management systems, to help ensure that threats posed by a constantly evolving environment are considered
- Review the alignment of the organization’s cybersecurity framework with regulatory expectations, new computing, hosting and storage capabilities (i.e., cloud), new “aaS” (as-a-service) business models, and global expansion
- Assess the implementation of revised technology security models, such as multi-layered defenses, enhanced detection methods, and encryption of data leaving the network
- Evaluate personal data breach and broader incident response planning

Cyber trend (continued)

Internal audit strategies are critical as technologies evolve and business environments change

Use of data and analytics in internal audit

08

Example focus areas for internal audit:

- Examining current processes to identify activities and projects in which data analytics and/or automation could provide efficiencies
- Evaluating higher risk business processes to identify whether or not data analytics could facilitate transparency and oversight

Cyber trend

Internal audit strategies are critical as technologies evolve and business environments change

09 Transitioning to and operating in the cloud

Example focus areas for internal audit:

- Review management's business case for the cloud solution to determine that benefits have been clearly defined and are measurable, as well as review management's subsequent plans and results for measuring and reporting on the benefits achieved
- Ensure threat modeling and risk assessments are performed and security requirements are developed and integrated within implementation plans and day-to-day operating procedures
- Participate in the company's vendor selection process to help ensure cloud vendors are able to meet the company's security, control, and legal/regulatory compliance requirements
- Periodically review the compliance posture of the cloud service providers (i.e., conduct on-site audit, review third-party audit reports, etc.) to determine whether the cloud service provider maintains an acceptable level of controls
- Review management's plan to monitor the usage of cloud services, including the plan for security monitoring and insider threats/abuse
- Review existing policies and procedures to determine suitability for cloud-based deployments and operations, and evaluate management's plan for business continuity and disaster recovery for the cloud operations (e.g., participate in business continuity disaster recovery exercise)
- Evaluate the organization's change management and business readiness plans around the implementation of the cloud solution
- Assess management's approach to designing and implementing controls to help ensure control efficiency and effectiveness, and an appropriate ration of automated to manual controls
- Review and provide recommendations on the organization's or department's new target operating model, particularly where new cloud solutions are replacing on premise systems and technologies

Wrap-up

- Cyber attack is high risk and it is not going away anytime soon
- When auditing/reviewing Cybersecurity: PEOPLE, PROCESS, and TECHNOLOGY
- Trend (High Risk Areas): Third Party Risk and Insider Threat

Thank you

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.