KPMG

# Cyber Security & Insider Threats

January 2018

# Agenda

- History and Types of Cyber Threats
- Issues Facing Cyber Security
- Cyber Security Trends and the Evolving Threat Landscape
- How do we Organize our Cyber Program?
- Q & A

| **Forbes Insights and KPMG 2017 Cyber Survey** | |
|---|---|
| **What would your organization need the most to be more effective in cyber security?** | |
| Stronger processes | 27% |
| More technology | 22% |
| Better strategy | 21% |
| Increased funding | 19% |
| Better quality staff | 7% |
| More staff | 4% |

KPMG

# History and Types of Cyber Threats

# A Brief History of Cyber Threats

## 1980s

- The Internet is a closed off world dominated by academics and hobbyists
- "White Hat" and "Black Hat" hackers emerge
- Hacking has recreational and educational purposes, but other motivations prevail and the Internet loses some of its innocence

## 1990s

- In the mid-1990s the Internet starts to reach mainstream consumers
- As more businesses come online, sensitive and financial data becomes a criminal commodity. Denial of Service (DoS) attacks emerge
- The first incident of cyber espionage is reported in the late 1990s

## 2000s

- The Internet becomes a regular part of life for most people and an accepted part of business and government activity
- More sophisticated cyber attacks come online such as financial Trojans and the hijacking of millions of online banking sessions coupled with dramatic increases in data breaches
- The rise of smartphones makes mobile the new frontier of cyber risks
- The first allegations of military cyber attacks occur in Estonia (2007) and Georgia (2008)

## 2010 to Present

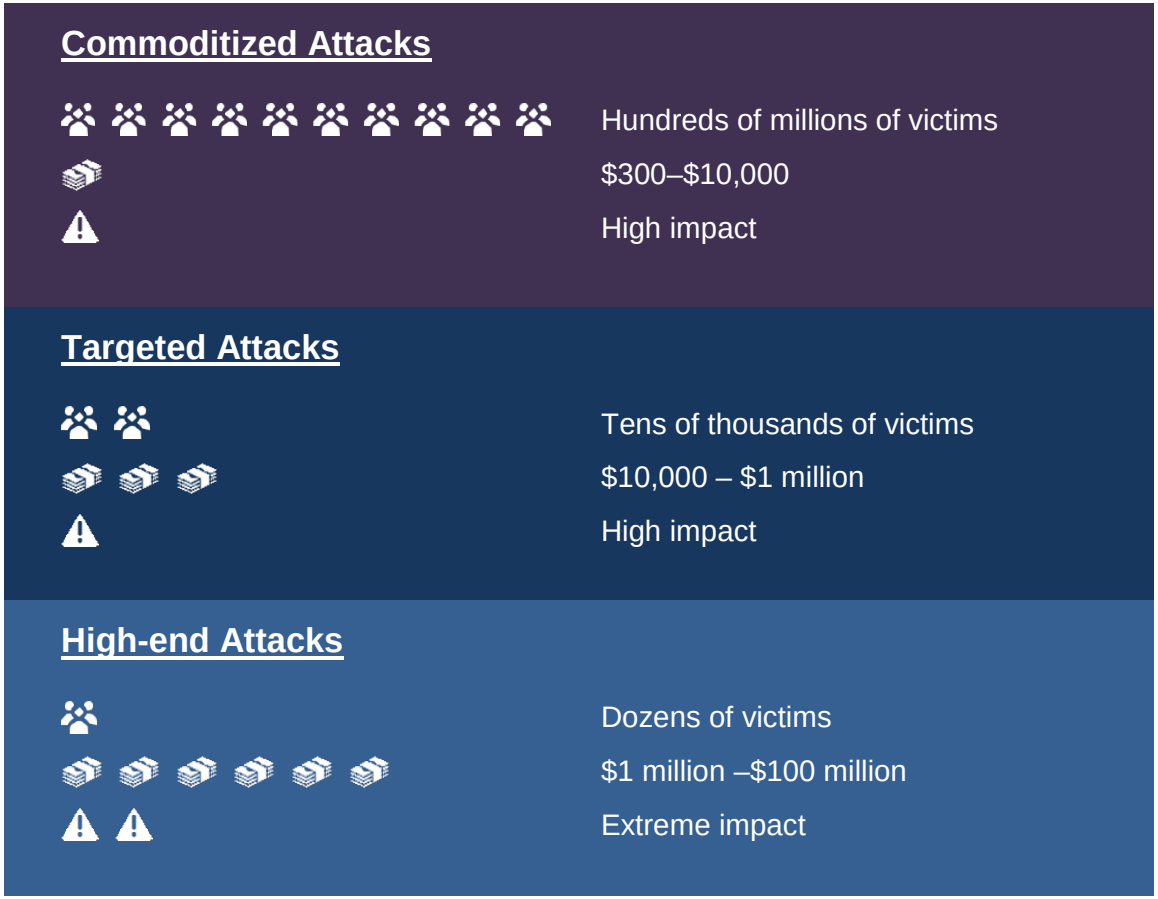
- The battle between cyber criminals and cyber security firms reaches maturity
- Cyber security is a $75 billion market place
- A black market thrives between cyber criminals where high-end exploitation tools can change hands for up to a million dollars
- Cyber criminals cost businesses $400 billion annually
- The Internet of Things (IoT) is likely the  to become the new cyber battleground

***Sources:*** Lloyd's, "Closing the Gap: Insuring your Business Against Evolving Cyber Threats" (June 2017)

KPMG

# Cyber Risks Today

- Businesses today are confronted by a bewildering variety of cyber attacks. This often makes cyber risks feel overwhelming.
- Analysis shows that attackers tend to be clustered into three main groups, using either “commoditized”, “targeted” or “high-end” approaches to victim selection and exploitation.




***Sources:*** Lloyd’s, “Closing the Gap: Insuring your Business Against Evolving Cyber Threats” (June 2017)

# Commoditized Attack Details

**Attackers:**

Organized crime groups operating internationally. Smaller - scale criminals. Hacktivists.

**Victim Numbers:**

Hundreds of millions.

**Technical Ability:**

Generally low. Attackers rely on an assortment of specialist tools designed by others and available in the online cybercriminal marketplace.

**Attack Methods:**

"Spray and pray" techniques, using spam emails, malicious website "watering holes" that target a group of people from a certain organization or geography, and criminal infrastructure to leverage vulnerabilities in often out-of-date software.

**Victims:**

Wide range of individuals and businesses, often via their customers.

**Financial Cost:**

$300 - $10,000.

**Overall Impact:**

High. Although returns may be relatively low, these economy-of-scale attackers monetize millions of victims and damage many more.

***Sources:*** Lloyd's, "Closing the Gap: Insuring your Business Against Evolving Cyber Threats" (June 2017)

# Commoditized Attack – Common Tactics

| Financial Trojans | Commodity Ransomware | Denial of Service Attacks | SQL Injection |
|---|---|---|---|
| — Malicious software<br>— Email attachment or web link delivery<br>— Allows attackers to hijack and modify a customer's online banking transactions | — Malware<br>— Locks victim's computer or mobile device<br>— Demands a ransom payment to regain access<br>— Often uses encryption to lock files forever if the user declines payment | — Disruption to online services<br>— Overloads networks and servers with attack traffic<br>— Commonly extortion-based | — Web software<br>— Allows SQL injection<br>— Attacker can smuggle commands into databases to destroy or modify company data or passwords |

***Sources:*** Lloyd's, "Closing the Gap: Insuring your Business Against Evolving Cyber Threats" (June 2017)

# Targeted Attack Details

**Attackers:**

Organized crime groups operating internationally.

**Victims:**

High-net-worth individuals and businesses, often targeted through their supply chains and customers.

**Victim Numbers:**

Tens of thousands.

**Financial Cost:**

$10,000 - $1 million.

**Technical Ability:**

Generally high. Attackers will deploy customized and targeted attack tools against commercial systems.

**Overall Impact:**

High.

**Attack Methods:**

Demonstrate an understanding of the industry they are attacking, including its systems and communications, and often causing significant business disruption by tailoring the attack to the victim, thus ensuring greater impact and financial rewards.

***Sources:*** Lloyd's, "Closing the Gap: Insuring your Business Against Evolving Cyber Threats" (June 2017)

# Targeted Attack – Common Tactics

| Repurposed Banking Trojans | Business Email Compromise Fraud | Targeted Ransomware |
|---|---|---|
| — Harvests and indexes victim data<br>— Installs remote access tools<br>— Allows targeted access to ultra high-net-worth entities' online devices<br>— Diversifying to target less mature sectors, including online retail customer accounts | — Also known as CEO fraud<br>— Misleads financial controllers, treasurers and payment clerks<br>— Triggers fraudulent payments<br>— Often pretends to be from CEOs or other senior executives<br>— Methods rely on social engineering and open-source research of the victims, together with poor email integrity | — Custom ransomware<br>— Targets critical systems and data stores<br>— Uses knowledge of commercial system vulnerabilities<br>— Aims for maximum impact and disruption to ensure large ransom payments from businesses<br>— Vulnerabilities exist across government and other sectors<br>— Education and healthcare are currently the targets of choice |

***Sources:*** Lloyd's, "Closing the Gap: Insuring your Business Against Evolving Cyber Threats" (June 2017)

# High-End Attack Details

**Attackers:**

Often smaller-scale, highly covert, organized crime groups operating internationally..

**Victim Numbers:**

Dozens.

**Technical Ability:**

Generally high. Attackers will understand the vulnerabilities and design a customized attack methodology.

**Attack Methods:**

Conceived from a specialist viewpoint with insider knowledge and understanding. These attackers develop their own custom toolkits to target software vulnerabilities. While their attacks can sometimes be easily recognized as the work of a particular group, in many cases the true motification remains unknown.

**Victims:**

Financial systems and infrastructure, through inside and specialist knowledge.

**Financial Cost:**

$1 million - $100 million.

**Overall Impact:**

Extreme – the damage to reputation and financial costs will permanently affect a business.

***Sources:*** Lloyd's, "Closing the Gap: Insuring your Business Against Evolving Cyber Threats" (June 2017)

# High-End Attack – Common Tactics

| Breaking into Banks and Financial Systems | Disrupting Critical Infrastructure |
| --- | --- |
| — Highly lucrative attacks<br>— Aimed at “weak links” | — Hallmarks of an Advanced Persistent Threat (APT)<br>— Common euphemism for state-sponsored cyber espionage techniques<br>— Often aimed at critical national infrastructure |

***Sources:*** Lloyd’s, “Closing the Gap: Insuring your Business Against Evolving Cyber Threats” (June 2017)

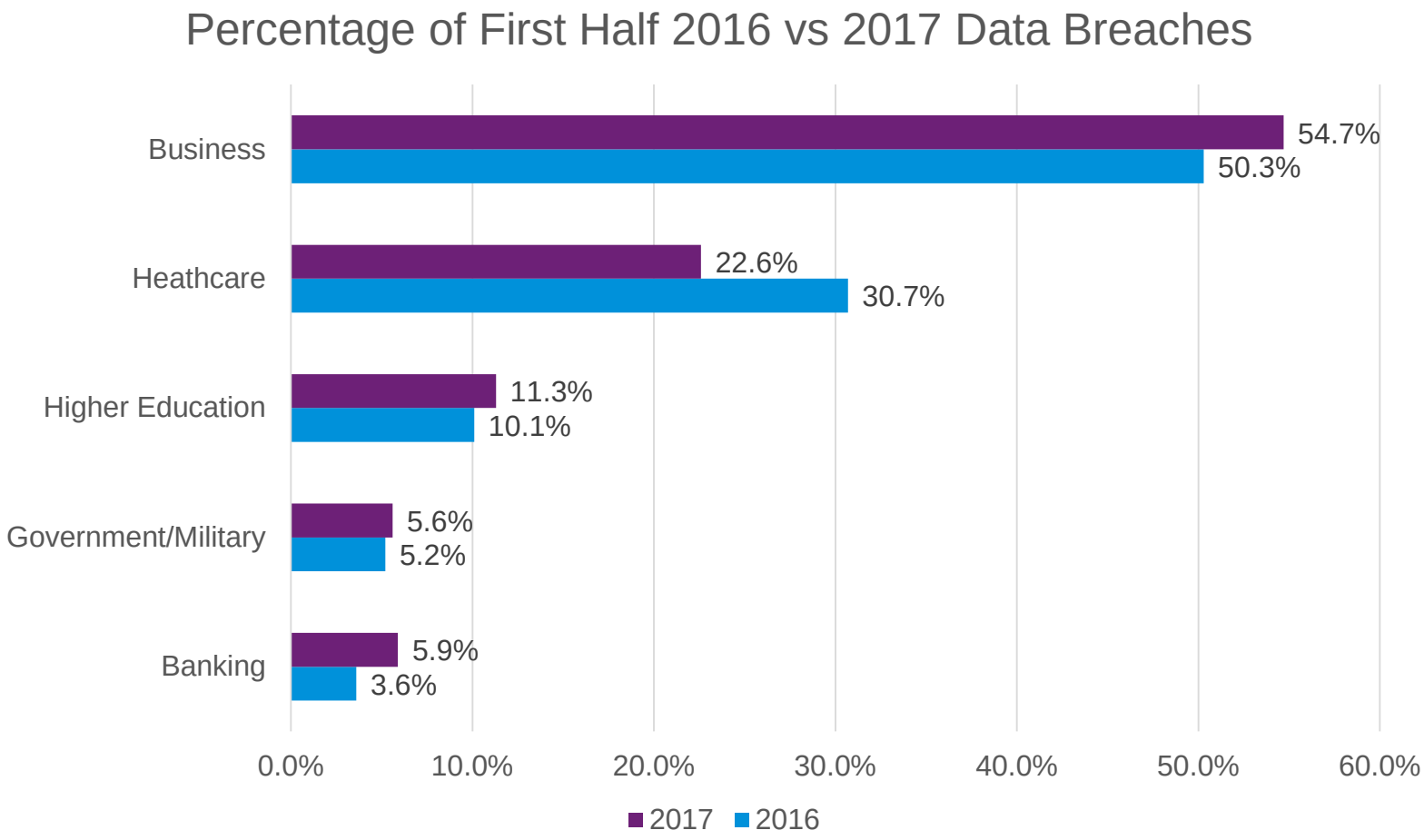
KPMG

# Issues Facing Information Security

# Top 5 IT Issues 2017

1. **Information Security**
2. **Stronger Policies and Procedures**
3. **Data-Informed Decision Making**
4. **Strategic Leadership/Governance**
5. **Sustainable Funding/Technology Investments**

# US Breaches By Industry Sector




***Sources:*** Identity Theft Resource Center, "At Mid-Year, U.S. Data Breaches Increase at Record Pace" (July 2017)

# Value of Sensitive Data

**Sensitive Data is easy to obtain and has a high resale value:**

- A stolen medical identity has a $50-$365 street value – more effort to obtain, more value to consumer
- Stolen social security number or credit card number only sells for $1 – high volume available, easy to detect and stop use
- Medical ID theft occurs when one person steals another's medical information to obtain or pay for health care treatment. According to the World Privacy Foundation, medical identity theft has affected 1.5 million Americans at a cost of more than $30 billion.
- Avi Rubin, Director of the Johns Hopkins University Health and Medical Security Lab, said the ***healthcare sector was the "absolute worst" in terms of cyber security.***
- ***"Malicious actors want as much intelligence as they can get, and healthcare is the easiest attack surface for seasoned and non-seasoned hackers."*** (James Scott, co-founder and senior fellow at the Institute for Critical Infrastructure Technology (ICIT) in Washington D.C.)
- According to the latest Verizon Data Breach Report, there were 620 data breach incidents in the manufacturing sector in 2016. Hackers largely targeted the manufacturing industry in order to steal trade secrets, business plans and valuable intellectual property.

# Audit Committee Research and KPMG

**AC Focus Area**

- **55%** of Audit Committee respondents feel that they should devote **“more time” or “significantly more time”** on Cyber for their agenda

**Cyber Oversight**

- **50%** of Boards have assigned Cyber oversight responsibilities to the Full Board or Audit Committee
- Organizations with structured leadership and strategy reduce average per record cost of a breach by **$6.59/record lost**)

**Brand Damage**

- Loss of customer data can result in reputational risk and organizational brand damage (Companies average **$3.32 million** in brand damage per breach)

**Training & Awareness**

- Organizations must invest in Cyber training and awareness for All employees, **including C-Level Executives**. It only takes **One employee** opening an email attachment to open the door for cyber criminals

# KPMG's Healthcare Cyber Security Survey

- 80% have reported a breach in the past 12 months
- 53% of Providers and 66% of Payers consider themselves ready for a cyber attack
- Only 13% say they are tracking attacks every day on their infrastructures.
- 27% do not have a dedicated security leader and 45% do not have any Security Operations Center (SOC) capability
- ***Our conclusion: Most of the industry is able to identify and react to yesterday's threats, not the new normal***

*233 Healthcare Executives (Payers and Providers) surveyed. 44% were Not-for-profit organizations. All had revenue over $500 million, 70% had revenue over $1 Billion.*

## The top seven causes of information security breaches:

1. **Naive end users**
   Lack of security awareness training and accountability
2. **Misconfigurations or human errors**
3. **Malicious software**
   viruses, worms and trojans
4. **Lost or stolen computers**
   including mobile devices
5. **Disgruntled Employees and Contractors**
6. **Came into focus of mass media**
7. **Insufficient funding**
   of IT and Information Security

# KPMG's Healthcare Cyber Security Survey

- Of the top seven reported causes of a security breach, five are people or process based.
- According to a recent HIMSS security survey:

"The greatest security threat to patient data is that it will be compromised by an organization's staff. Eighty (80) percent of respondents noted that they were concerned that human-related factors would put data at risk. Furthermore, respondents were most likely to indicate the greatest motivator leading to the compromise of data is for workforce members to snoop on co-workers, friends and neighbors patient information".

## The top seven causes of information security breaches:

1. **Naive end users**
   Lack of security awareness training and accountability
2. **Misconfigurations or human errors**
3. **Malicious software**
   viruses, worms and trojans
4. **Lost or stolen computers**
   including mobile devices
5. **Disgruntled Employees and Contractors**
6. **Came into focus of mass media**
7. **Insufficient funding**
   of IT and Information Security

KPMG

# Cyber Security Trends and the Evolving Threat Landscape

# Current Cyber Security Trends

Extortion-driven attacks and **ransomware** attempts will increase and will become more threatening (moving in to backups, more theft, etc.)

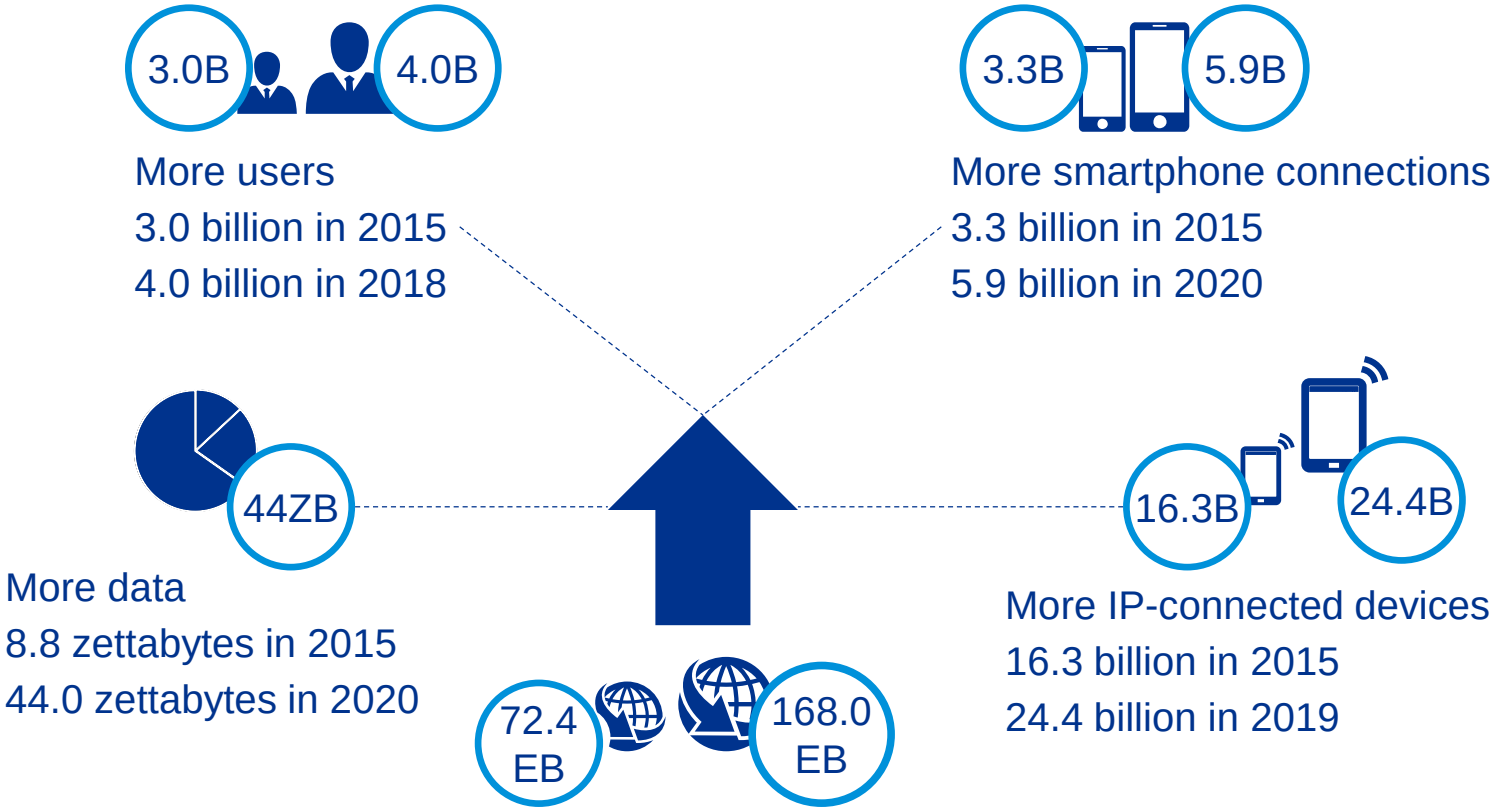
**EMR interoperability** will provide larger attack surface, requiring new thinking and solutions, such as **blockchain**, patient ownership of data, etc.

Widespread use of **medical devices** and **IoT** (internet of things) brings a parallel increase in risk

**Insider threat** will be brought into greater focus as technology improves, allowing visibility into credential abuse

Organizations will focus much more on risks posed by **third-party vendors** and **suppliers**

# New Platforms Mean New Threats




***Sources:*** McAfee Labs (2015)

# Who is Doing It?

Cyber threats are malicious activities carried out via digital means.

There are generally 5 types of attackers:

**THE INDIVIDUAL**

— Motivated by revenge, notoriety, or profit. Can be either an individual external to the organization or within it.

**ORGANIZED CRIME**

— Motivated solely by financial gain.

**NATION – STATE**

— Motivated by improving geopolitical position or commercial interests.

**HACKTIVISTS**

— Goals include attacking or disrupting to further a political agenda.

**CYBER TERRORISTS**

— Goals include destroying critical infrastructure to further a political agenda.

# Current Cyber Security Landscape

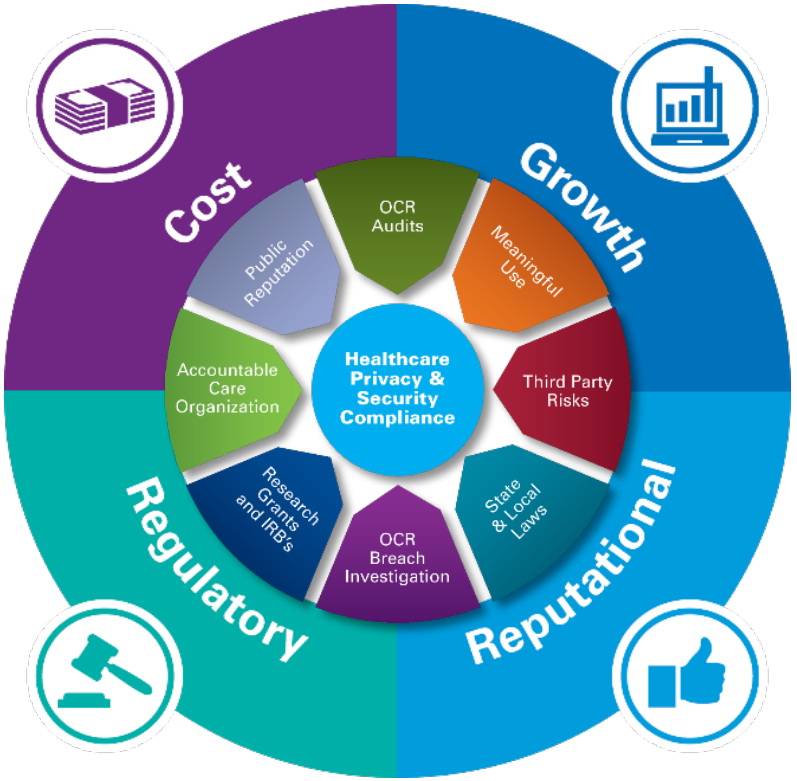
**Adversaries are getting more advanced**

The number of endpoints and the amount of sensitive data that needs to be protected is **exponentially increasing**

The business continues to grow into new digital businesses in**creasing pressure on IT and security**

**New cyber regulations continue to challenge** organizational focus

**Cyber spend is reducing as cyber fatigue sets with the board**, which is focused on the reduction of cyber and reputational risk



# Do We Have Our Eyes Open?

**More than half** of organizations say it is unlikely or **highly unlikely that they would be able to detect** a sophisticated attack. (iTreasurer)

Once detected, it can take **months** to resolve a breach (Verizon)

Data production will be **44 times greater** in 2020 than in 2009 (IDC) making analysis and monitoring even more difficult

For most companies, it takes **over 6 months** to even realize they have been breached. (Ponemon)

**Only 31%** of organizations discovered they were breached through their own resources - Most entities are **informed of a breach by third-parties** such as law enforcement, etc. (Mandiant/FireEye)

In recent years, the percentage of companies affected by a successful cyberattack is **71%** (NetIQ)

In 60% of cases, attackers were able to compromise an organization **within minutes** (Verizon)

Just 55% of organizations feel they have adequate resources for handling security incidents (KPMG Healthcare Survey)

…There is a growing deficit between how quickly attackers can compromise vs. how quickly organizations can detect and respond. *In other words, Attackers are improving faster than defenders…*

# Ransomware Attacks

- Ransomware attempts increased 4X in 2016 relative to 2015 and expected to double again in 2017 vs. 2016 (SC Magazine)
- 40% of spam email contained ransomware (IBM)
- Healthcare and Financial Services hardest hit Industries due to their dependence on business-critical information (Malwarebytes)
- Ransomware is increasing in popularity and complexity due to its ease of use and profitability for hackers.
- According to a new Healthcare IT News and HIMSS Analytics Quick HIT Survey, about 50% of all hospitals that responded said they suffered from a ransomware attack. Another 25% said they were unsure or had no way of knowing.
- Most business face at least 2 days of downtime but less than 25% of victims actually report it (the Atlantic)

# Recent Events

- Hacker incidents now account for about one-third of the 183 breaches added to the wall of shame so far this year (2016). But they represent about 84 percent of the 12.9 million individuals affected by the breaches added.
- A large credit reporting agency reported that hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers for over 143M consumers.
- 80M records taken from a large Healthcare payer.
- A California University indicated that 80,000 university personnel may be at risk following a cyber attack on a university system storing social security and bank account numbers.

- A Pennsylvania University revealed that hackers had breached an estimated 18,000 student and faculty accounts and an additional 500 research partner accounts. The attack targeted the university's College of Engineering.
- 400 hospitals billings delayed as clearinghouse hit with ransomware.
- A major accounting and consulting firm reported a major cyber attack that compromised its email system and client records

KPMG

# How do we Organize our Cyber Program?

# The New Normal

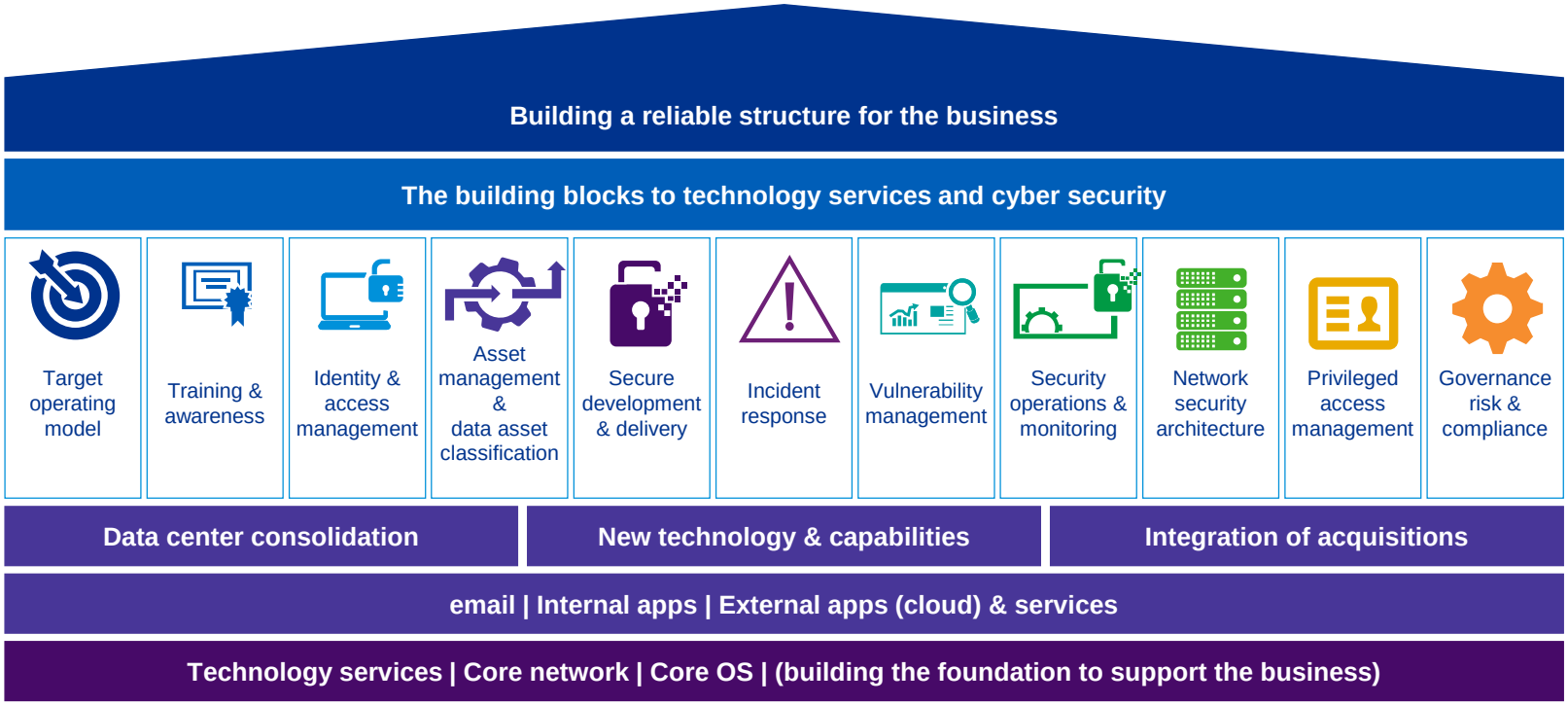
**Based on KPMG's experience, industries are facing unique challenges.**

- The **evolving threat landscape**, where cyber attacks today are more sophisticated and well-funded given the increased value of the compromised data on the black market.
- Organized criminals are remotely breaking into IT systems, stealing sensitive information for identity theft or fraud.
- The **adoption of digital records** and the automation of systems
- The **ease of distributing sensitive data** both internally (laptops, mobile devices, thumb drives) and externally (third parties, Cloud services).
- Shared services, outsourcing, and cloud solutions increase risks for data loss.

# Building a Cyber Program with the Business

Organizations universally agree: Cyber resource and investment allocations must be balanced between traditional reactive security measures, more proactive business enablement, and advanced sustainability objectives.

| Cyber Defense | Business Enablement | Resilience |
|---|---|---|
| Cyber defense includes actions and infrastructure intended to defend the perimeter. | Business Enablement involves cyber teams working collaboratively with business owners. | Resilience represents an organizational commitment to cyber maturity. |



# Why Do Organizations Get It Wrong?

**Themes from organizations that have got it wrong:**

- Not linking security to the business strategy
- Failing to build in security fundamentals, comprehensive security testing, and asset management creates a weak foundation
- Failing to get the basics right such as configuration and patching – security is additive so new challenges must be combined to existing challenges
- Not keeping up-to-date with the latest threats and evolving their security awareness around it
- Not considering global security compliance and regulation
- Not completing appropriate third party due diligence
- Concentrating too much on prevention of security incidents and not enough on detection of incidents and appropriate reaction to incidents
- Believing that traditional security controls are enough in our organizations. Today's enhanced security risk landscape requires intimate and immediate knowledge of threats, assets, and adversaries
- A lack of planning for the unexpected such as a major Crypto or other significant security architecture component failure: the heartbleed vulnerability had been there for years and was a simple two line coding error. There will be others, the only questions are where and when
- Allowing new functions or applications to be written in different programming languages to existing systems, on different machines, by different teams
- Failing to consider sustainable security
- Failing to deal with a breach immediately and completely – following a security breach expect a significant increase in targeting

KPMG

# Cyber Maturity Lenses

**Legal and compliance**

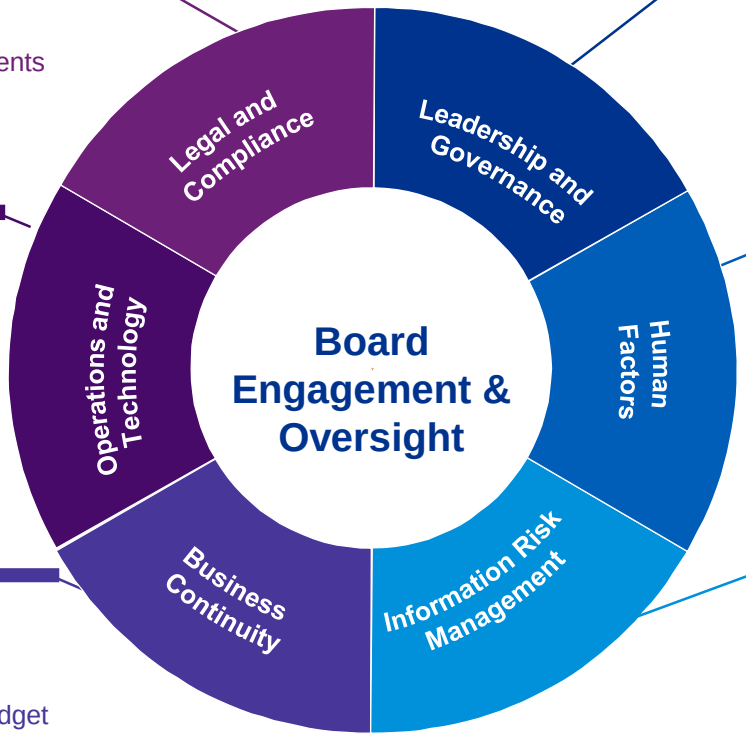
- Inventory of compliance requirements
- Compliance program components
- Role of the audit committee
- Litigation inventory
- Cyber insurance

**Operations and technology**

- Threat and vulnerability management
- Logical security controls
- Physical security controls
- Security monitoring
- Incident response
- Integration with IT service management

**Business continuity and crisis management**

- Ability to manage cyber event
- Financial ramifications and budget
- Resources required and training
- Detailed plans
- Communications
- Testing




**Leadership and governance**

- Board involvement
- Third party supplier relationships
- Identification of critical data
- Ownership and governance for data protection
- Project management

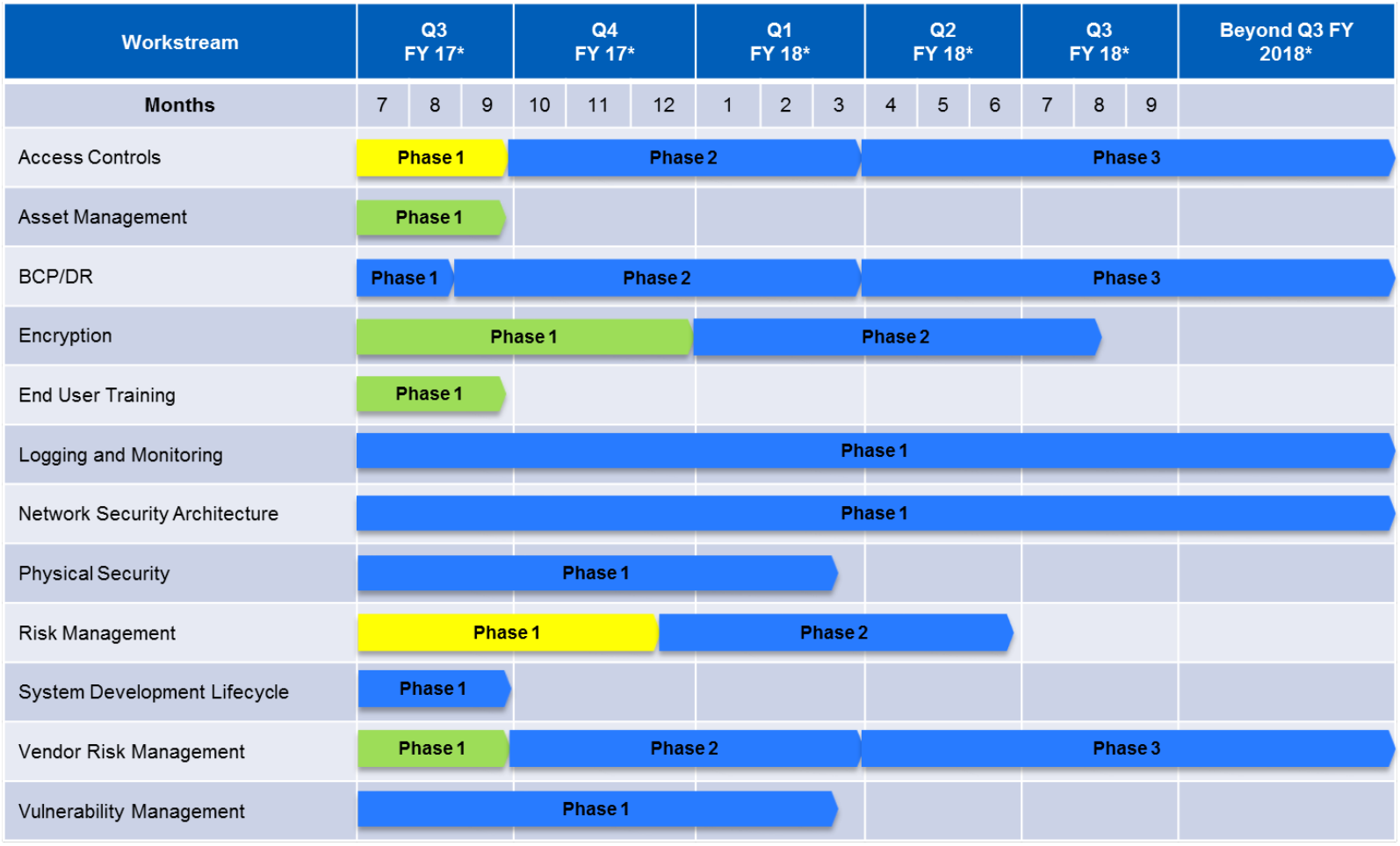
**Human factors**

- Training and awareness
- Culture
- Personnel security measures
- Talent management
- Organizational roles and responsibilities

**Information risk management**

- Risk management approach and policies
- Risk tolerance identification
- Risk assessment and measures
- Change management
- Information sharing
- Third party accreditation
- Information communication architecture

# Cyber Remediation Plan




KEY: Not yet started | In Progress | Completed

* As defined by CLIENT XXX

# Project Charters

## Objectives

- Build and mature the Security Operations Center (SOC) to detect, analyze, respond to, report on, and prevent incidents.

## Scope

- Cyber threat intelligence
- Log management
- Sensor platforms (IDS/IPS, SIEM)
- Alert triage
- Incident response
- Forensics

## Outcomes / Capabilities

- Real-time monitoring and triage
- Cyber intel collection and analysis
- Trending, long-term analysis
- Incident analysis and response coordination
- Countermeasures implementation
- Forensic artifact handling and analysis

## Tasks: Stage 1 – Short Term

**Phase 1 – Complete Technology Evaluation & Plan Project**

- Prepare project plan and define key engagement milestones.
- Identify the business and IT stakeholders that will be involved as part of the assessment.
- Communicate project schedule and objectives to involved parties.
- Schedule and conduct a kickoff meeting for the key stakeholders identified.

## Tasks: Stage 2 – Near Term

**Phase 1 – Monitoring Use Case Development**

- Conduct and facilitate workshops as needed with Information Security, operations teams, and key stakeholders to better understand the data, systems, applications, and network segments that are considered critical;
- Review CLIENT XXX operating models as they related to the business and IT to better understand sources of risk and how they may be leveraged by threat actors;
- Review threat actor activity as it relates to the Healthcare vertical and creation of the threat landscape and threat actor model that will drive use case selection and the SOC Target Operating Model.

# Call to Action

**New threat model**

- Organizations have to align their security programs to the new threat model
- Full attention should be paid to the insider threat as well as the external attacker

**Compliance does not equal cyber maturity**

- Organizations need to assess cyber maturity against a more rigorous standard, not just regulatory compliance
- Integrate cyber security with compliance to drive organization wide initiatives
- Stronger reporting structure for the TOM (target operating model) and responsibility to not just the CIO but also to Compliance and the board

**Security threats are not confined to your own organization**

- Organizations have to improve their communications both internally and externally
- Integrated cyber security technologies, with strong reporting and monitoring capabilities

**Increase cyber Investments – In the right order**

- We need to invest in cyber security across the paradigm of people, process and technology
- Only invest in technology with a measurable plan!
- Attend to the basics first, build the right foundation before trying to advance

KPMG

# How do we integrate Cyber into ongoing IA activities?

# IT Internal Audit & Cyber Approach

**Where to Start:**

— **Use of IT Frameworks**

- Use of IT frameworks helps to ensure coverage over various IT general and Cyber areas.
- Frameworks to assist in determining “what” can be evaluated.
- Existing IT frameworks may need additional controls from frameworks such as examples: ISO 27001/2, NIST 800-53, NIST CSF, Cloud Security Framework, Payment Card Industry Security Standards.
- usually a combination of multiple frameworks plus regulatory requirements.

— **Update the IT Universe and Risks to Include Cyber**

- Updating of the risks and universe via ongoing review, continual relationship management, and relationships with IT including the integration of cyber security solutions and processes

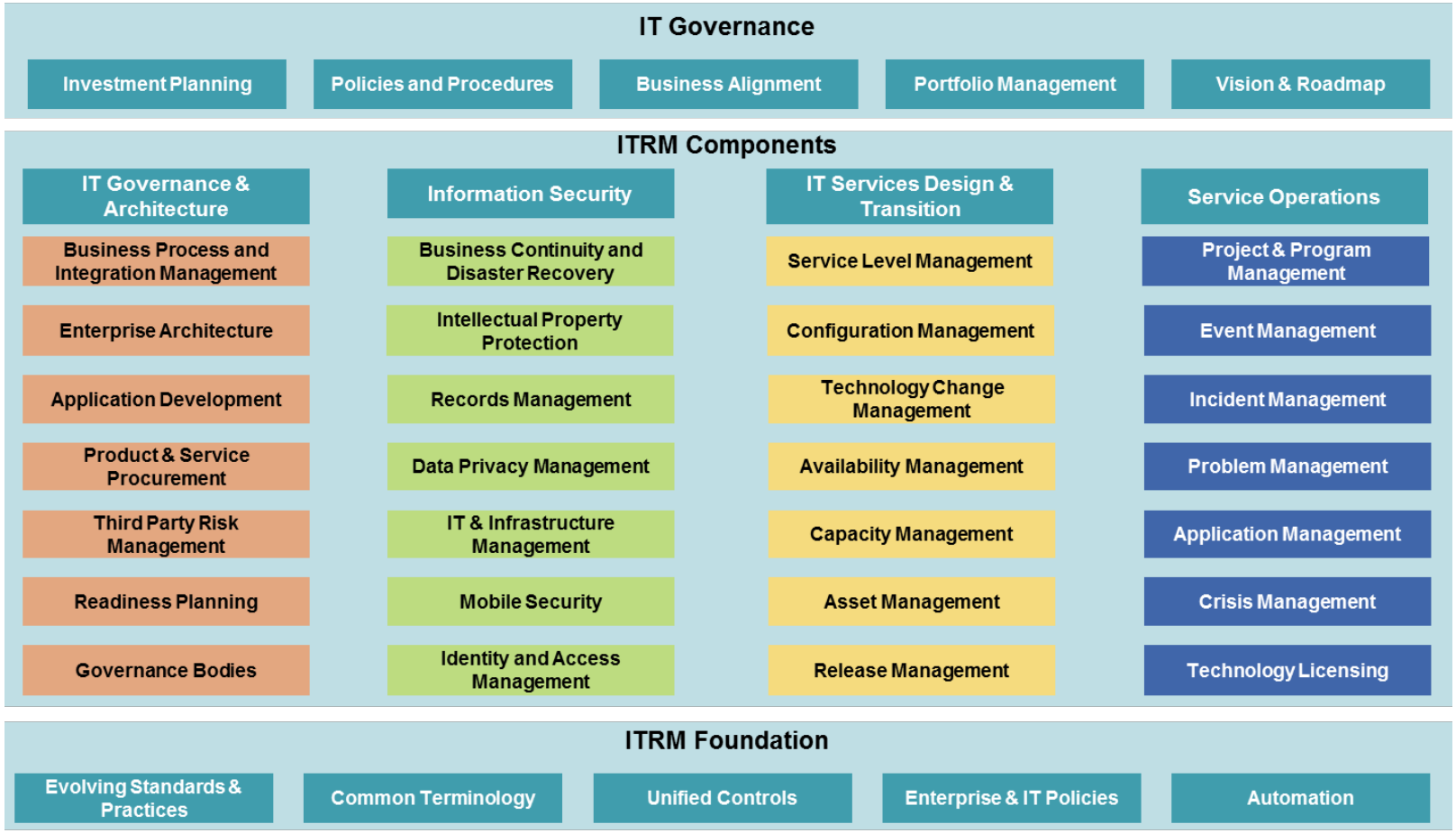
— **Annual Planning / IT Risk Assessment**

- Define as part of your annual defining of risk and audits areas relating to cyber for assessment
- Breaking audits into 1) Required audits (SOX, Compliance) 2) Operationally critical testing and risk assessment input, (consider on a rotation taking into consideration cyber security risk and emerging technology risk), 3) Assurance audits over projects (typically ERP, implementation, major security initiatives)

— **Team / Skills to Perform Cyber Audits**

- Do we have the experience or training in cbyer to perform cyber audits
- Use of IT specialist in testing; can be accomplished through IT guest auditor, external resources, and also consider an approach to use specialist resources and audit generalist for knowledge transfer

# Sample IT Risk Framework



# Framework - Risk Management Domains

—IT typically organizes delivery through technology domains/towers; adopting a risk-centric lens across each domain, ITIA can audit risks in an organized manner

—Sample IT Risk domains below are based on leading standards such as COBIT, ITIL, NIST and should be tailored to the organization

| # | IT Risk Domains | Sample IT Risk Sub-Domains | | Sample Key Risks |
|---|---|---|---|---|
| 1 | IT Strategy & Architecture | — Strategic Mgmt.<br>— Organisation<br>— Architecture Mgmt. | — Emerging/Disruptive Technologies<br>— Risk and Compliance | — Enterprise architecture not matching the strategic goals of the organization can affect scalability and limit business growth<br>— Failure to consider current and emerging technologies for product development can affect competitiveness in the marketplace. |
| 2 | Portfolio, Programme & Project Management | — Portfolio Mgmt<br>— Programme Mgmt | — Project Mgmt | — Lack of a thorough understanding of business needs can impact quality (perceived and actual) of IT services delivered to the business.<br>— Slow or poor quality delivery of business transformation can affect competitiveness in the marketplace. |
| 3 | Application Management & SDLC | — Application Management<br>— Coding Standards<br>— Release Mgmt | — SDLC<br>— Testing/QA | — Inconsistent definition or application of SDLC standards across the IT organization can lead to issues in production and impact service delivery to the business<br>— Failure to consider risk and security within application development practices can increase the likelihood of business disruption from cyber threats. |
| 4 | Service Delivery/IT Operations | — Capacity Mgmt<br>— Change Mgmt<br>— Configuration Mgmt<br>— Incident Mgmt | — IT Asset Mgmt<br>— Knowledge Mgmt<br>— Patch Mgmt<br>— Problem Mgmt | — Underutilization of IT's capabilities through poor resource allocations, structural inefficiency or strategic misalignment can lead to increased costs and diminished service in operational environment.<br>— Poor responsiveness to production outages can lead to a loss of revenue and increase operational costs. |
| 5 | IT Service Continuity | — Business Continuity<br>— Disaster Recovery | — Systems & Service Availability | — Failure to understand and design for business resilience expectations can increase damages in the event of a disaster |
| 6 | Cyber/Information Security | — Application Security<br>— Data Protection<br>— Identity & Access Mgmt | — IP Protection<br>— Physical Security<br>— Vulnerability Mgmt | — Inadequate information security capabilities can expose the enterprise to data loss resulting in financial and reputational loss.<br>— Lack of data encryption systems, processes and infrastructure can significantly increase the likelihood of losing intellectual property. |
| 7 | Data Management | — Data Governance<br>— Big Data | — Data protection & Backup<br>— Records Management | — Inability to understand and utilize enterprise (Inc. external) data can affect competitiveness in the marketplace. |
| 8 | Supplier Management | — Contract Management<br>— Out-sourcing/Off shoring | — Third party (general) | — Inadequate definition and enforcement of IT supplier contracts can lead to business disruptions.<br>— Inadequate due diligence performed on third party prior to formal engagement. |
| 9 | IT Business Management | — Financial Mgmt<br>— Talent Mgmt<br>— Stakeholder Engagement & Comms | | — Lack of transparency of IT costs, benefits and risk can negatively impact business perception of IT.<br>— Poor customer experience with IT can lead to lower adoption and reduced ROI for businesses.<br>— A lack of mature, comprehensive and effective IT Risk Management framework can lead to a loss of control over business processes and delivery. |

# IT Audit and IT Risk Universes

- Gather systems in the universe and the risks in order to develop the basis for the IT audit program
- Both can be gathered from information available via the IT organization as well as interviews and surveys
- IT Universe - Some of the best information can be pulled from IT management systems such as Configuration Management Databases (CMDBs), security tools such as vulnerability scanners, and system management tools like those from ServiceNow or IBM
- IT Risks may also be gathered via Enterprise Risk Management (ERM) processes or Disaster Recover / Business Resiliency planning documents – consider "What Could Go Wrong"

## IT Risk Universe

| Business Continuity and Disaster Recovery | Data Management | Data Privacy | IT Governance |
|---|---|---|---|
| Backup and recovery capabilities | Accuracy and integrity of data | Customer data | Application governance |
| Business continuity plans | Business intelligence capability | Employee personal identifiable information | Business process governance |
| Business involvement | Data availability | Encryption | Controls governance |
| Disaster recovery plans | ERP integration | Intellectual property protection | Demand management |
| Leadership and ownership of plans | | Ownership of data | Infrastructure governance |
| Roles and responsibilities | | Protection of sensitive data | Known deficiency remediation |
| Third-party considerations | | Removable storage | Policies and procedures |
| | | Unmonitored 3rd party access | System selection |

| IT Asset Management | Vendor Management and Sourcing | IT Infrastructure | Regulatory Compliance |
|---|---|---|---|
| Application obsolescence | Abiding by client standards | Infrastructure growth | e-Discovery |
| Data center physical security | Appropriate Use of vendors | Operating System | HIPAA |
| Hardware inventory management | Counterparty risk | Database | Local country laws/regulatory and statutory reporting |
| IT purchasing | Management of product quality | Network architecture | Payment card |
| Software asset management | Vendor contingency plans | System availability | Sarbanes-Oxley |
| Technology obsolescence | Vendor health | System maintenance | |
| | Vendor performance management | System software management | |
| | Vendor secured environment | Wireless computing | |

| IT Security | IT Strategy and Business Integration | Project and Change Management | Resource Management |
|---|---|---|---|
| Data and application classification | Acquisitions, Divestiture and JVs | Controls integration | Identification of needed skill sets |
| Logical data center security | Application system portfolio | Project management and execution | Institutional knowledge and key person dependency |
| Privileged users | Budget and IT investment | Project portfolio management | IT staff turnover |
| Provisioning and De-provisioning | Emerging technology | Significant projects and initiatives | Succession planning |
| Segregation of duties | IT cost take-out | System development lifecycle | Training and education |
| Use of encryption | Plant/site closures | | |
| Virus protection | Shared services | | |
| Vulnerability patching | Strategic alignment | | |

# IT Framework Aligned to Auditable Entities

| | | Business Capabilities Examples | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Auditable Entity (Audit Universe Area) | | Sample | Sample | Sample | Customer Inflight Experien | Sample Business Process | Marketing | Customer Relationship Ma | External Relationships and | Finance | Human Resource Manage | Information Technology | Legal | Procurement and Third Pa | Sales | Strategy |
| **IT Risk Domain** | **IT Risk Sub-Domain (Auditable Entity)** | | | | | | | | | | | | | | | |
| Technology Regulatory Compliance | PCI DSS Compliance | | 2018 | | 2018 | | | | | 2018 | | 2018 | | 2018 | | |
| | HIPAA Compliance | | | 2018 | | | | | | | 2018 | 2018 | 2018 | | | |
| | PII Compliance | | | | | 2018 | | | | | 2018 | 2018 | | | | |
| | Other | | | | | | | | | | | 2018 | 2018 | | | |
| Data Management | Data Governance | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 |
| | Data Quality | | | | | | | | | | | 2017 | | | | |
| | Data Platform and Architecture | | | | | | | | | | | 2017 | | | | |
| | Database Operations | | | | | | | | | | | 2017 | | | | |
| | Big Data - EDW Interface | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 | 2017 |
| Application Management & SDLC | Application Management | | | | | | | | | | | 2019 | | | | |
| | SDLC | | | | | | | | | | | 2017 | | | | |
| Information/ Cyber Security | Identity & Access Management - Privileged Access | | | | | | | | | | | 2017 | | | | |
| | Information Security Strategy and Governance | | | | | | | | | | | 2018 | | | | |
| | Identity & Access Management - IdM Replacement | | | | | | | | | | | 2017 | | | | |
| | Continuous Security Monitoring | | | | | | | | | | | 2018 | | | | |
| | Network Infrastructure - Security Review | | | | | | | | | | | 2017 | | | | |
| | Cyber Incident Response - eEnablement Control | | | | | | | | | | | 2017 | | | | |
| | Vulnerability Management | | | | | | | | | | | 2018 | | | | |
| IT Strategy and Architecture | Strategic Management | | | | | | | | | | | 2018 | | | | 2018 |
| | Risk Management | | | | | | | | | | | 2017 | | | | |
| | Architecture Management | | | | | | | | | | | 2019 | | | | |
| | Emerging/Disruptive Technologies - Social Media | | | | | 2017 | | 2017 | | | | 2017 | | | | |
| | Emerging/Disruptive Technologies - Cloud | | | | | | | | | 2017 | | 2017 | 2017 | 2017 | | 2017 |
| | Emerging/Disruptive Technologies - Digital Payments | | 2018 | | 2018 | 2018 | 2018 | 2018 | 2018 | 2018 | | 2018 | | | 2018 | |

KPMG

# Q & A

# Speaker Biographies

## Jason Lininger, KPMG IT Audit and Assurance

Jason Lininger is a Director in KPMG's Advisory Services practice with more than 20 years of information technology management experience in the areas of security management, compliance, cyber security, audit, and technology risk. He has a strong background across project and program management of IT risk, regulatory and compliance management, and strategic IT risk management. Jason's current and past clients include some of the leading entities in the financial services, retail, healthcare, utilities, diversified industrial products, consumer goods, public sector, and insurance industries. Jason has also served as the IT Internal Audit Director for a Fortune 500 organization and was responsible regionally for helping organizations develop their cyber risk management approach as part of a cloud security corporation.

## Melissa Lawlor, KPMG Cyber Services

Melissa is a Manager in KPMG's Cyber Practice and is part of KPMG's National HIPAA team where she serves as a National Quality Director for Healthcare Security. Melissa has strong experience in information security and healthcare regulatory compliance. Her expertise includes information security, security program strategy and design, privacy and compliance, cyber security and maturity assessments, and global regulatory standards based risk and security assessments (HIPAA, NIST SP 800-53, 800-30, 800-66, NIST CSF, and ISO 27001/27002).

## Michael Briggs, KPMG Cyber Services

Michael is a Senior Associate in KPMG's Cyber Security Services practice with experience in information security operations and regulatory compliance. Michael has served on multiple Cyber Security engagements for clients in manufacturing, healthcare, and life sciences. He has assisted with the construction and management of several security operations centers. His expertise includes information security, security program strategy and design, security operations center strategy, design and platform management, cyber security and maturity assessments, and global regulatory standards based risk and security assessments.

# Thank you


**Jason Lininger**
**Director Advisory,**
**IT Audit and Assurance**
**414-477-6265**
**jlininger@kpmg.com**

**Melissa Lawlor**
**Manager Advisory,**
**Cyber Security**
**215-298-4489**
**mlawlor@kpmg.com**

**Michael Briggs**
**Sr. Associate Advisory,**
**Cyber Security**
**928-606-7041**
**mjbriggs@kpmg.com**