The Growing Gap – Are you cyber prepared?

Rakesh Thakur

EY Americas Government & Public Sector Cyber Leader

Chris Brown

EY Government & Public Sector Cyber Leader

May 16, 2018

EY

Building a better working world

Cyber threats are emerging as a top priority for government entities worldwide

The number of government transactions going digital is expected to increase from **10%** in 2011 to about **33%** in 2020.

The **low cost of deployment** - executing a breach with **a US$20 piece of malware** - could cause large losses for organizations. **92% increase** in new downloader variant in 2017.

Rising sophistication is making existing technology obsolete. **46% increase** in new ransomware variants.

The number of **smart cities is** expected to quadruple globally from **21** in 2013 to **88** in 2025.

The use of **cloud services** among government agencies is on the rise (NSA and DoJ moved their IT infrastructure to cloud; Many US State Governments embracing cloud-first policy).

US$2.1 trillion
The cost of cybercrime to the global economy by 2019.

55 million
Voters records were hacked from the Philippines election commission database in 2016. 700k voter records were hacked from State of IL.

US$222 million
is the cost of NASA's drone that was hacked and the hackers tried to crash it into pacific ocean in 2016.

6,500
was the number of times various Ukraine government institutions were targeted by hackers during the last two months of 2016.

50 million
personal data records of Turkish citizens (two-thirds of the total population) were stolen in 2016.

Sources: Firstpost; The Washington Post; BBC; Symantec; BW Smart Cities; publictechnology.net; Reuters.

Significant challenges remain for governments on the regulatory and institutional aspects of cybersecurity

Issues	Indicators	
Lack of awareness and strong regulatory policies	**34%** of nations out of 193 countries have their national cybersecurity strategy in place.	**50%** Share of government versus private in applying patches to security flaws in software developed by Veracode.
Insufficient funds for cybersecurity services	**9% reduction** in funding for the US cyber command in FY16 that was US$463 million, compared with US$509 million in FY15	**< 2%** share of the information security spend as a percentage of total IT budget of US states.
Lack of human resources personnel with relevant skills	**1.5 million** shortage of cybersecurity professionals predicted to be across the globe by 2020.	**5% versus 10%** share for cybersecurity in total IT budget of US state and local government agencies versus commercial.

Sources: Infosecurity; White House website; govtech.com; Business Insider; PwC; CBRonline.com.

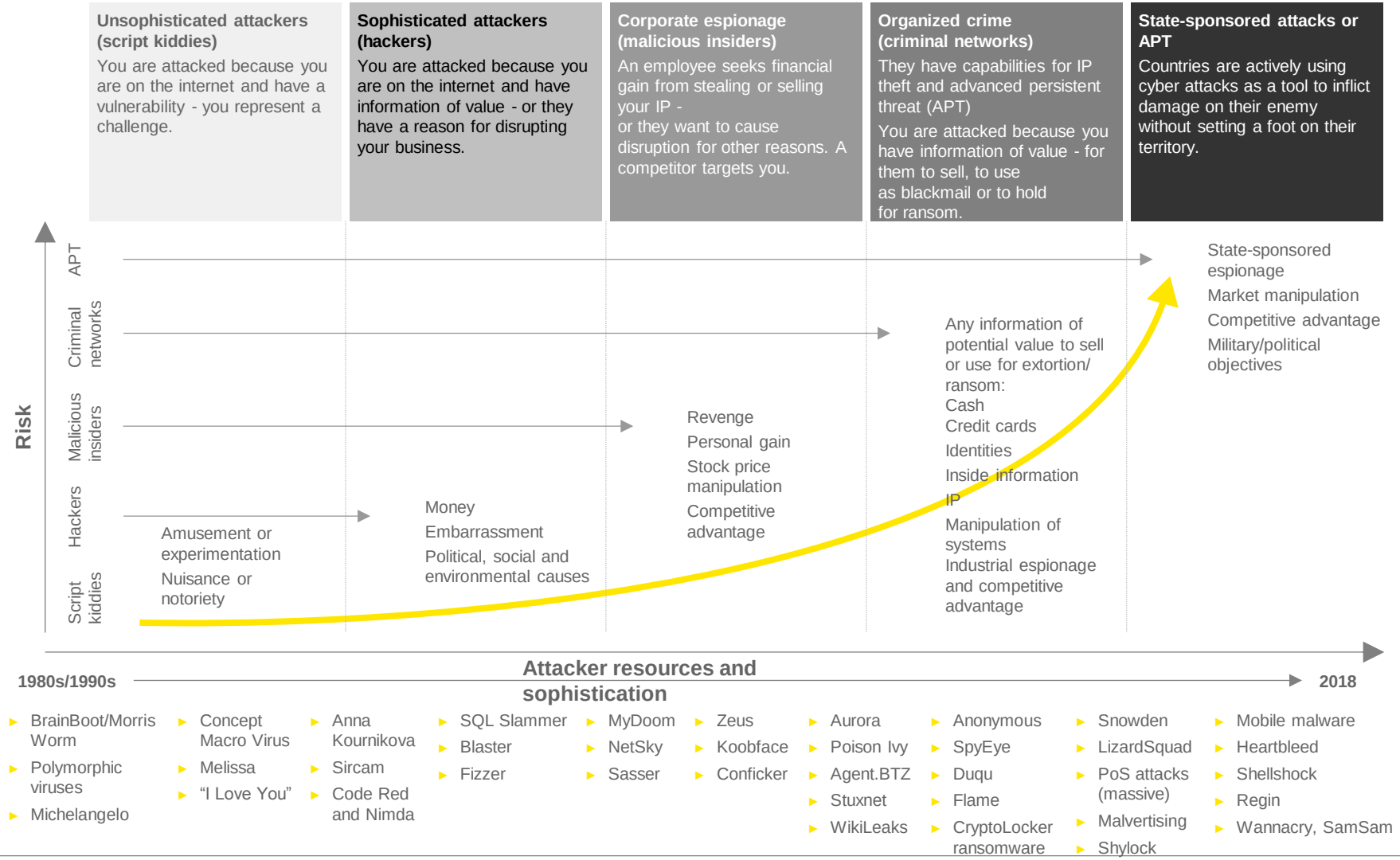
As governments increasingly face innovative threats, they must take a proactive stance on cybersecurity

Issues	Indicators	
Increasing complexity of cyber threats	**5.4B** WannaCry attacks blocked. 46% increase in new ransomware variants in 2017.	**US$81 million** was stolen from the Bangladesh Central Bank account maintained with US FED, through suspicious SWIFT* instructions in 2016.
Rise of the Internet of Things (IoT) will open up new avenues of cyber attacks	**70%** of the most commonly used IoT devices contain vulnerabilities.	**25%** of the total identified cyber attacks in enterprises will involve IoT by 2020.
Lack of holistic approach to tackle threat and difficult to defend targeted threats with common solutions	**3.5 million** teachers and other employees of a US public agency were accidentally published on the Internet.	**The US** has alleged that Russia interfered in their presidential election process by hacking US political sites and email accounts.

Sources: Govtech.com; Forbes; Reuters; CNN; Sonicwall.

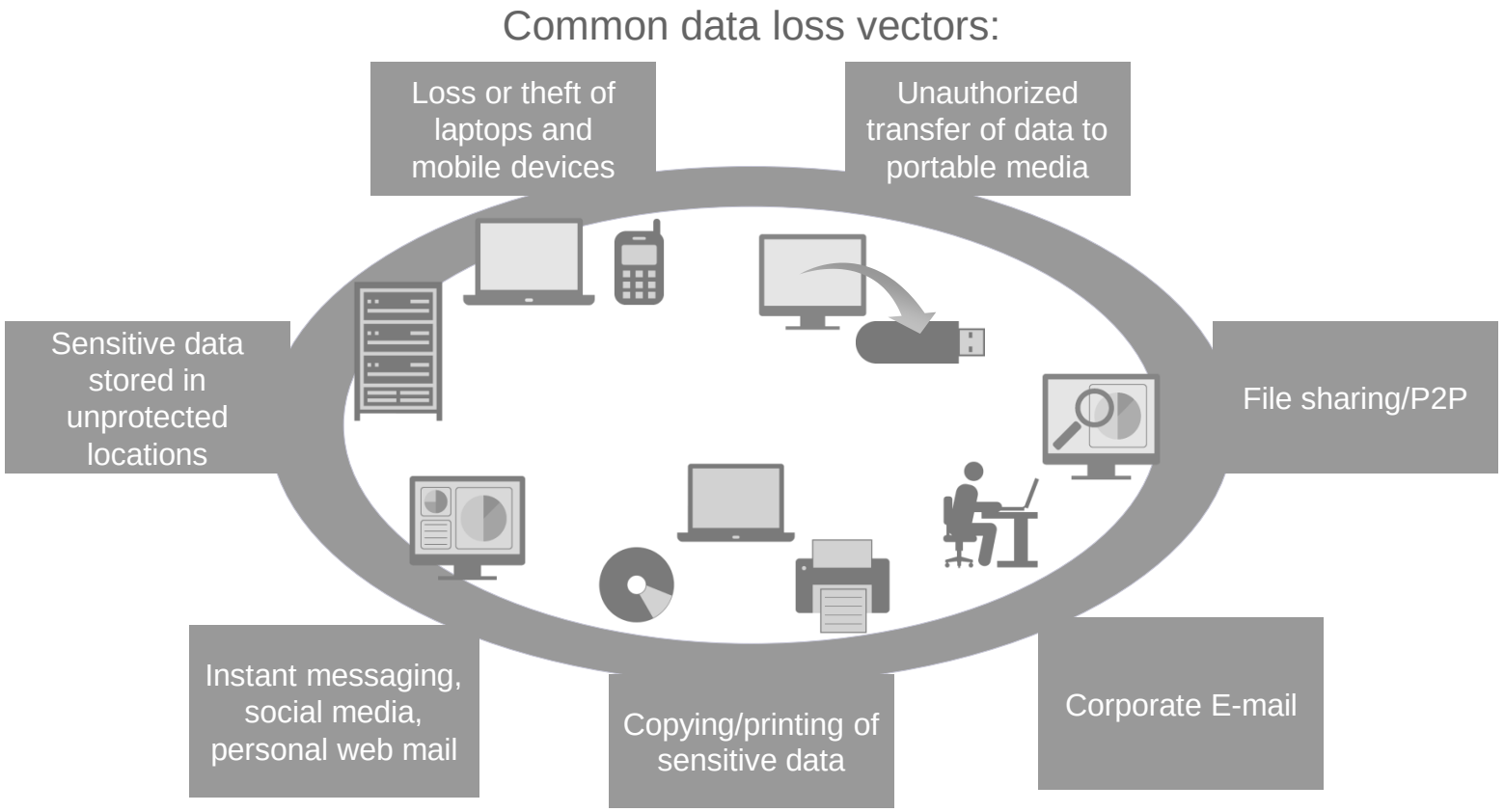
* SWIFT: Society for Worldwide Interbank Financial Telecommunication

Cybersecurity threats and attackers continue to evolve, transforming the risk for public sector agencies



Source: EY internal decks.

How Data can be lost without knowing about it?



A very complex problem

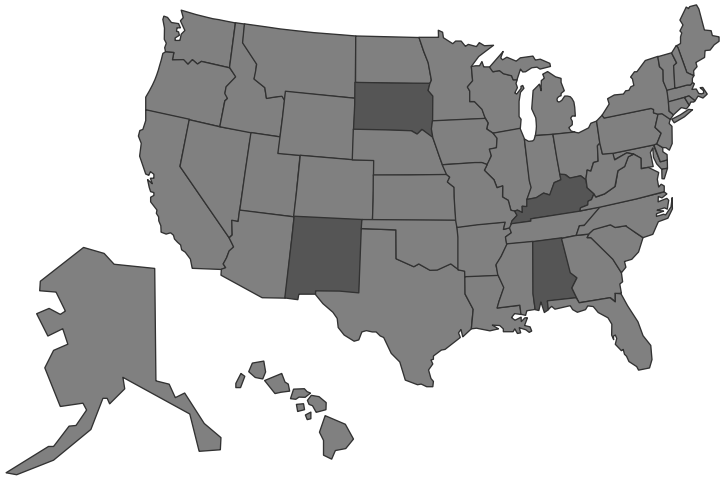
Program challenges:

- Difficulty in identifying all relevant data loss channels within the organization
- Complexity of information flows within the extended enterprise
- User capabilities to access, copy and send sensitive data outside of the company, including across borders
- Growing number and complexity of regulatory requirements to protect sensitive information, particularly for companies operating in many different states and internationally
- Lack of forensic / incident response capabilities to effectively respond to data loss and data breaches
- Encryption tools allow malicious users to hide their activity from most DLP technology

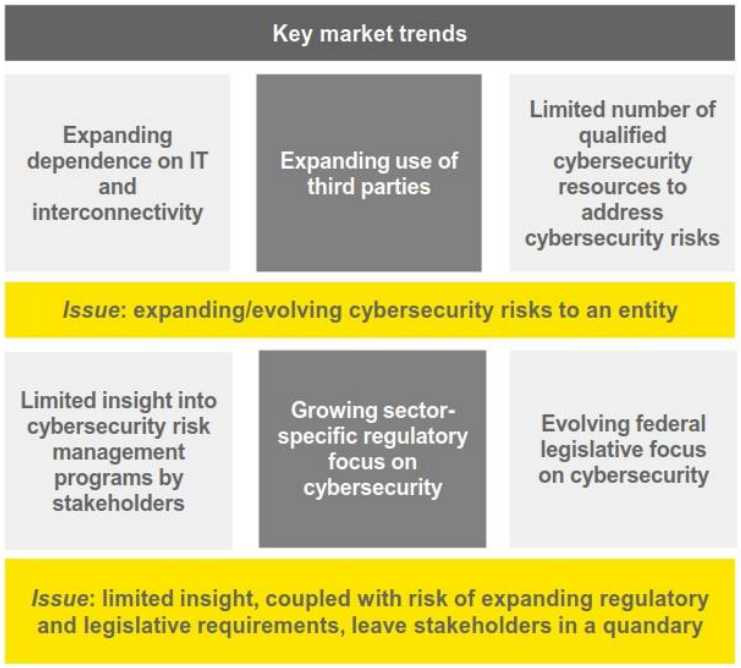
Fundamental questions to answer:

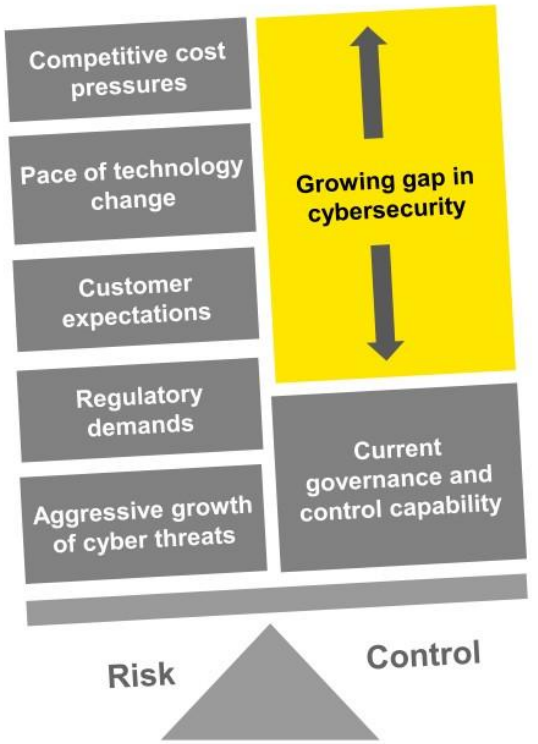
- What sensitive data do you hold?
- What is your highest risk sensitive data considering personally identifiable data, customer data and intellectual property?
- Where does your sensitive data reside, both internally and with third parties?
- Where is your data going?

States with data privacy laws:



Cybersecurity trends and its impact



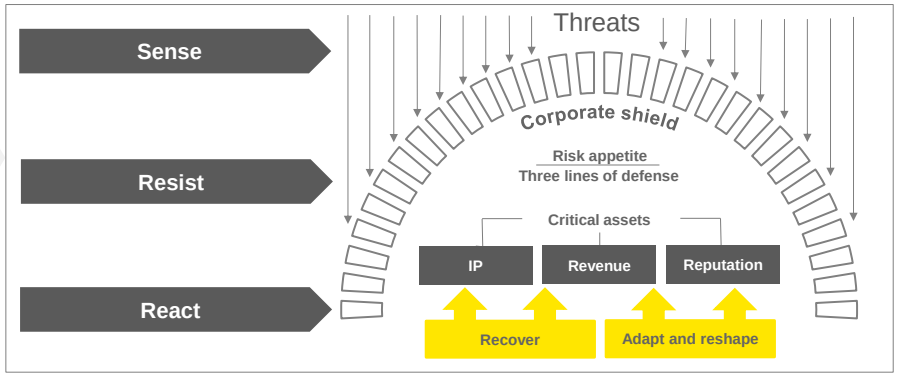


What can you do?

EY Global Information Security Survey focuses on improving cyber resilience of organizations through a three-stage framework …

Government organizations are making progress in improving the way they respond to today's cyber threats and attacks, but there is a need for considerable improvement in the way they sharpen their **senses**, upgrade **resistance** to attacks and **react** better to post-attack situations.

Cyber resilience framework



Sense is the ability of organizations to predict and detect cyber threats. Government organizations need to use cyber threat intelligence and active defense to predict what threats or attacks are heading in their direction and detect them when they do, before the attack is successful.

Key findings (GPS) "sense"

59%

of respondents mentioned that their organization does not have a security operation center (SOC).

64%

would not increase their cybersecurity spending after experiencing a breach which did not appear to do any harm.

71%

do not have, or only have an informal, threat intelligence program.

53%

doubt that they are going to be able to continue to identify suspicious traffic over their networks.

… that helps them to work toward improving their cybersecurity capabilities

Resist mechanisms are basically the corporate shield. It starts with how much risk an organization is prepared to take across its ecosystem.

Key findings (GPS) "resist"

88%

of respondents do not think that their information security function is meeting the needs of the organization.

95%

of organizations do not evaluate the financial impact of every significant breach.

43%

of responders this year are saying their budgets increased over the last 12 months.

76%

of respondents mention that lack of skilled resources is one of the key challenges for smooth operation of information security operations.

React: if sense fails and there is a breakdown in resist, organizations need to be ready to deal with disruption, ready with incident response capabilities and ready to manage the crisis.

Key findings (GPS) "react"

70%

of respondents rated business continuity management as their joint top priority, alongside data leakage/data loss prevention.

35%

say they would issue public statement to the media within the first week while investigations continue.

49%

do not have an agreed communications strategy or plan in place in the event of a significant attack.

6%

of responders have recently made a significant change to their organization's strategy and plans.

Establish an open, stable and secure cyberspace with focus on three key agendas

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.

How EY's Global Government & Public Sector can help your organization
Around the world, governments and not-for-profit organizations are continually seeking innovative answers to complex challenges. They are striving to provide better services at lower costs and to create sustainable economic development, a safe environment, more transparency and increased accountability. EY combines private sector leading practices with an understanding of the public sector's diverse needs, focusing on building organizations' capabilities to deliver improved public services. Drawing on many years of experience, we can work with you to help strengthen your organization and achieve lasting improvements. Our Global Government & Public Sector brings together teams of highly skilled professionals from our assurance, tax, transaction and advisory services. We are inspired by a deep commitment to help you meet your goals and enhance public value, for today and tomorrow.

EYG no. XXXXXX

BMC Agency
GA 1007012

ED None

ey.com