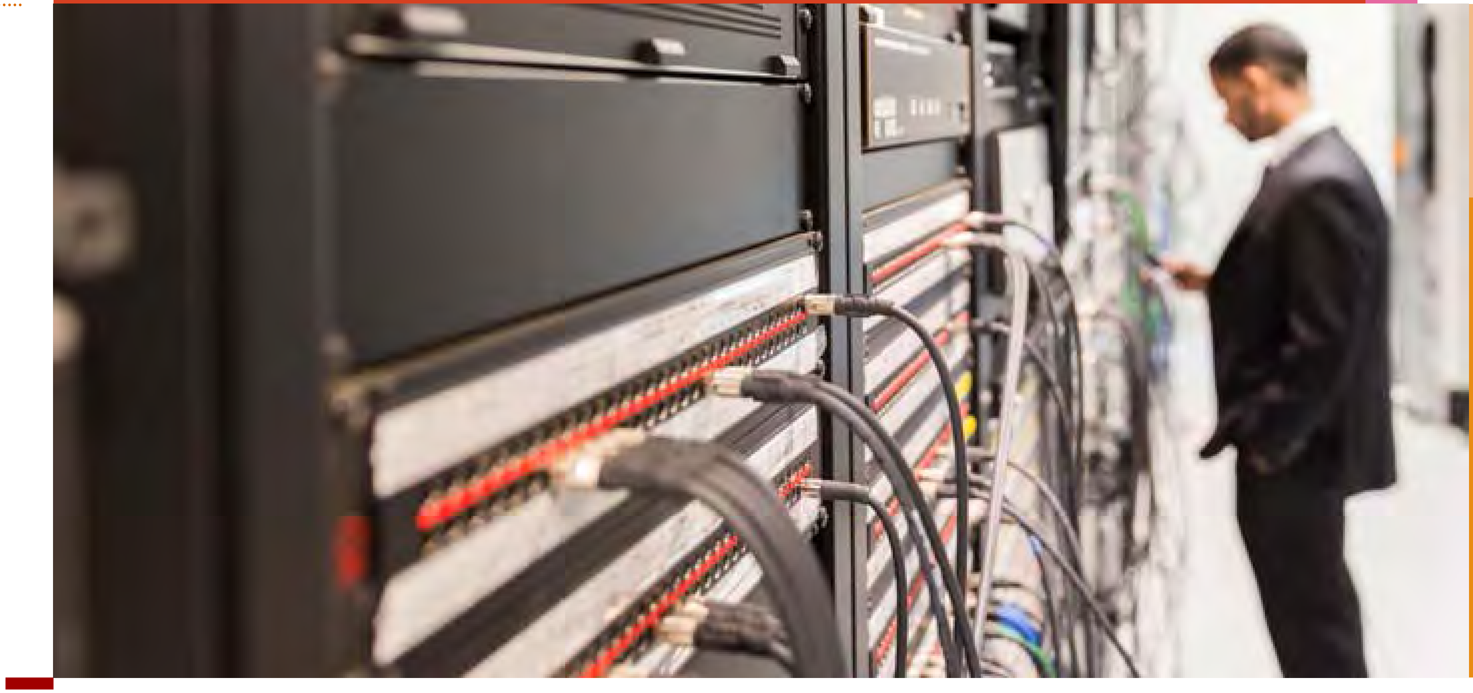
Advisory

PwC Nigeria
Cybercrime Event

Strictly Private
and Confidential
FINAL

17 November 2013



pwc

Welcome

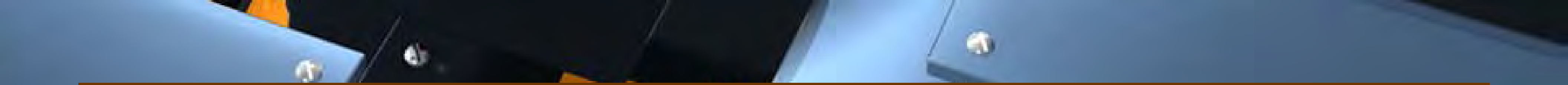
Agenda

Time	Activity	Speaker(s)
8.30-9.00am	Arrival	All
9.00 – 9.15 am	Opening address	Ken Igbokwe
9.15 – 10.00 am	Key note address– Industry trends and outlook	Dr. Ademola Odeyemi
10.00 – 10.45am	Overview of the cyber threat landscape	Neal Pollard/ Femi Tairu
10.45 – 11.15 am	Tea Break	All
11.15 – 12:30 pm	Interactive Session - Through the Eyes of an Attacker Case Study: Cyber attack at a major financial services firm Q&A: Cyber threats, counter measures and challenges	Neal Pollard/ Femi Tairu/Conference Participants
12:30 – 12:45 pm	Recap and closing	Daniel Asakpokhai
12.45 - 2.30pm	Lunch One-on-one meetings	All

Opening Remark

Dealing with Cybercrime threat in the Financial Services sector

A keynote presentation by Dr Demola Odeyemi,
E.D. Guaranty Trust Bank
November 2013



Outline

1. Introduction
2. How big is the threat?
3. Estimated cost of Cybercrime
4. Types of cybercrimes
5. Cybercrime attack groups
6. Prevention
7. Conclusion

Introduction:

Internet and emergence of alternative channels – the platform for Cybercrime

- Traditional banking was essentially paper-based.

- Since the turn of the 21st century (the birth of globalization and advanced technologies) banking has also caught the technology fever.

- In the financial services world of today, banking transactions are fast leaving the four walls of brick& mortar branches to the clouds.

- Transactions are now being done at the speed of thought.

- Increasing transactions are being done via ATM, POS, Internet banking, Mobile Money, NEFT etc

- Account opening is now possible on Social Media platforms such as Facebook

- 24 hour banking via Banks' online internet banking platforms is now possible

- Banks are now driving visibility via youtube, instagram, twitter, google+ etc

- Agent banking and virtual banking are now in the pipeline in Nigeria

- As a matter of fact, virtual banks like Ally bank (USA), First Direct (UK), Metro bank (UK) exist where all transactions are conducted online.

- This internet and rapid evolution of alternative platforms/channels for the provision of banking services pose significant threats to the financial services industry.

- Banks worldwide are custodians of customers' funds/assets which runs into trillions of dollars and billions of customer records – these are at risk!

How big is the threat?

Statistics across the globe

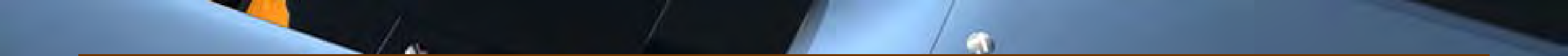
□59% of ex-employees admitted to stealing company data when leaving previous jobs.

□Cyber Crimes are growing and by 2017, the global Cyber Security market is expected to skyrocket to $120.1 billion.

□1 in 10 social network users said they'd fallen victim to a scam or fake link on social network platforms.

Top countries of cybercrime origination	
Source of Attack	Number of Attacks
Russia	2,402,722
Taiwan	907,102
Germany	780,425
Ukraine	566,531
Hungary	367,966
USA	355,341
Romania	350,948
Brazil	337,977
Italy	288,607
Australia	255,777

□The general distribution of cyber attack is as follows: 50% hacktivism, 40% cybercrime, 7% cyber espionage and 7% cyber warfare



How big is the threat?

a. €135,000

b. 2.7%

c. 49%

d. €29,954

e. 33%

f. 67%

g. 63% - of respondents believe their organization is only partially equipped, or do not consider their organization to have adequate measures to deal with cybercrime.

h. 57% - of respondents stated that no further actions were taken following an investigation of internal or external incidents.

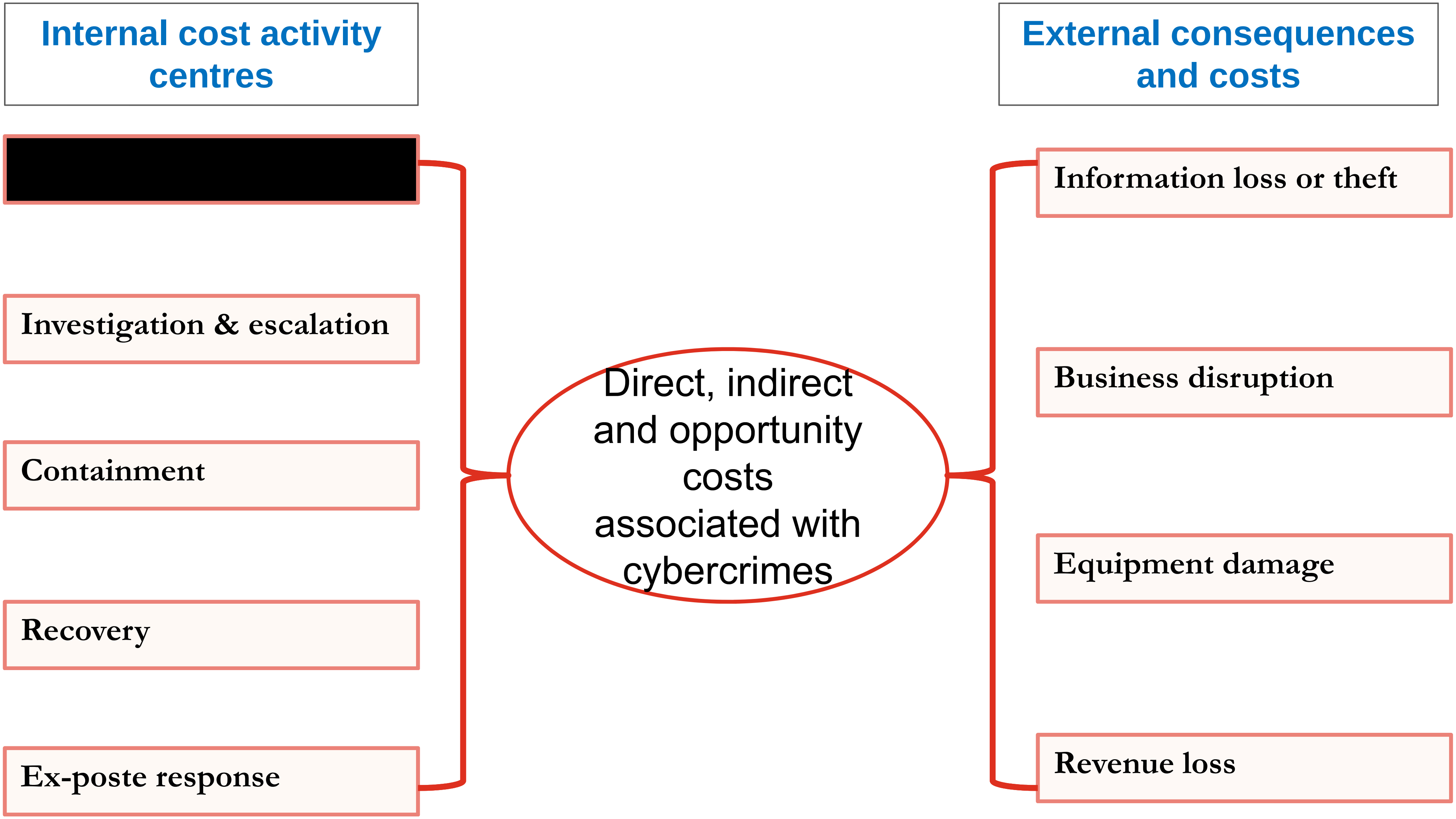
i. 30% - of respondents believe that evolving technical threats present the biggest challenges in information security.

j. 76% - are of the view that existing policies only partially address or fail to address recent business and technology changes.

***Courtesy: Deloitte* Irish Information Security and Cybercrime Survey 2013**

Estimated cost of cybercrime

Costing framework for Cybercrime



Internal cost activity centres

[redacted]

Investigation & escalation

Containment

Recovery

Ex-poste response

Direct, indirect and opportunity costs associated with cybercrimes

External consequences and costs

Information loss or theft

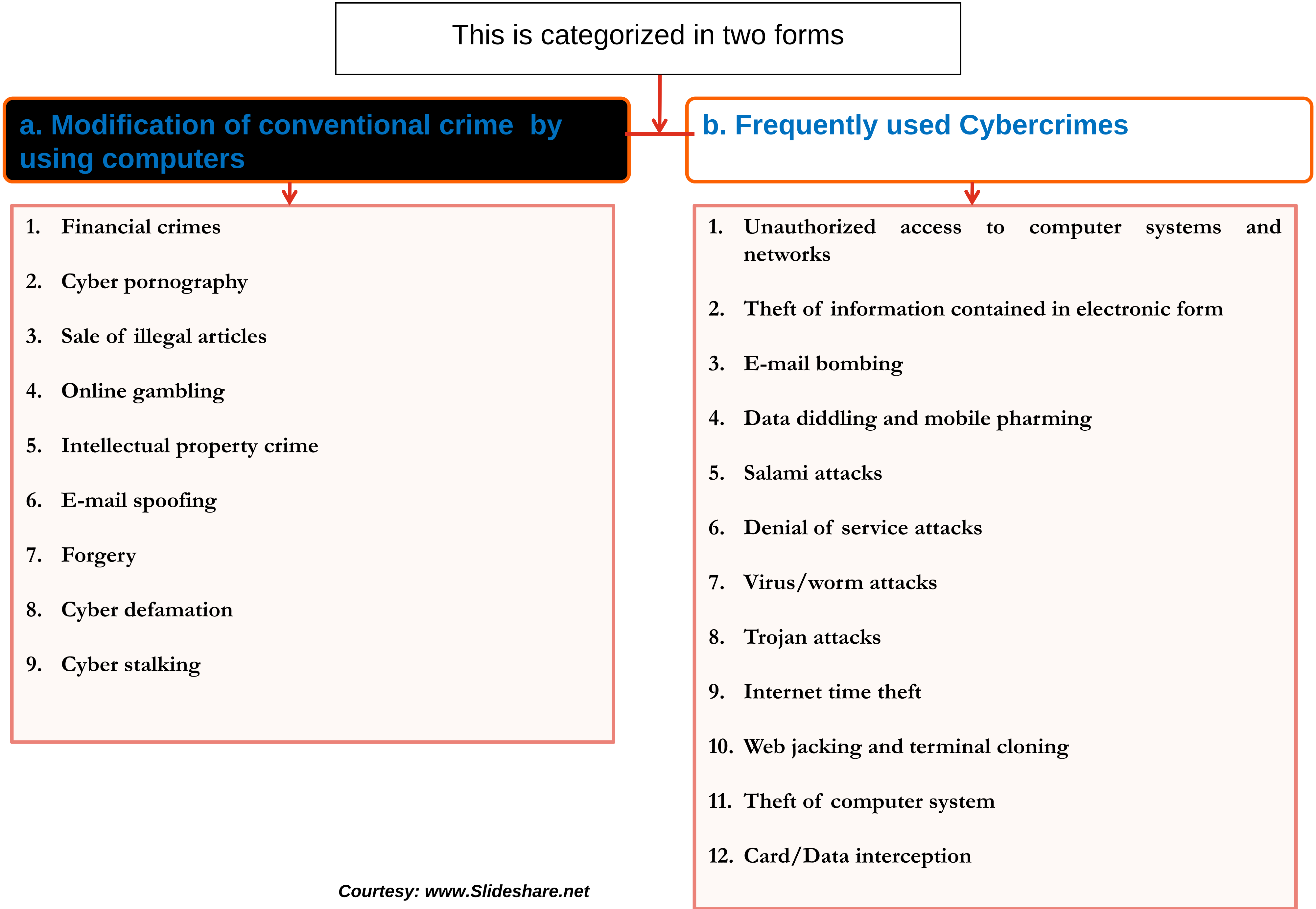
Business disruption

Equipment damage

Revenue loss

Courtesy: Ponemon Institute

Types of cybercrimes



This is categorized in two forms

a. Modification of conventional crime by using computers

1. Financial crimes
2. Cyber pornography
3. Sale of illegal articles
4. Online gambling
5. Intellectual property crime
6. E-mail spoofing
7. Forgery
8. Cyber defamation
9. Cyber stalking

b. Frequently used Cybercrimes

1. Unauthorized access to computer systems and networks
2. Theft of information contained in electronic form
3. E-mail bombing
4. Data diddling and mobile pharming
5. Salami attacks
6. Denial of service attacks
7. Virus/worm attacks
8. Trojan attacks
9. Internet time theft
10. Web jacking and terminal cloning
11. Theft of computer system
12. Card/Data interception

Courtesy: www.Slideshare.net

The cybercrime attack groups

Teenagers (ages 9 – 16yrs)

Organized hacktivists

•Banks' fears have traditionally been provisioning arising from Bad loans.

•Loan loss expenses are to a large extent predictable based on the loan exposure amount.

•But the financial loss from cybercrime is absolutely unpredictable.

Unlike Loan loss expense, it has no cap. This is the emerging threat to banks' financial performance (Profitability)

Corporate espionage

Disgruntled employee

Prevention of cybercrime

Conclusion

- While loan loss expense used to be the biggest threat to banks, cybercrime is the emerging and potentially biggest threat of the future.

- Cybercrime has left the subsistence level, it is now being perpetrated on a commercial scale by very organized, well-connected and sophisticated professionals and even firms

- Cybercrime has overtaken drug-trafficking as the biggest illegal revenue generator for people of the underworld

- Collaboration (domestic and cross-border) among players and regulators in the global financial services industry is very important in fighting the threat of cybercrime.

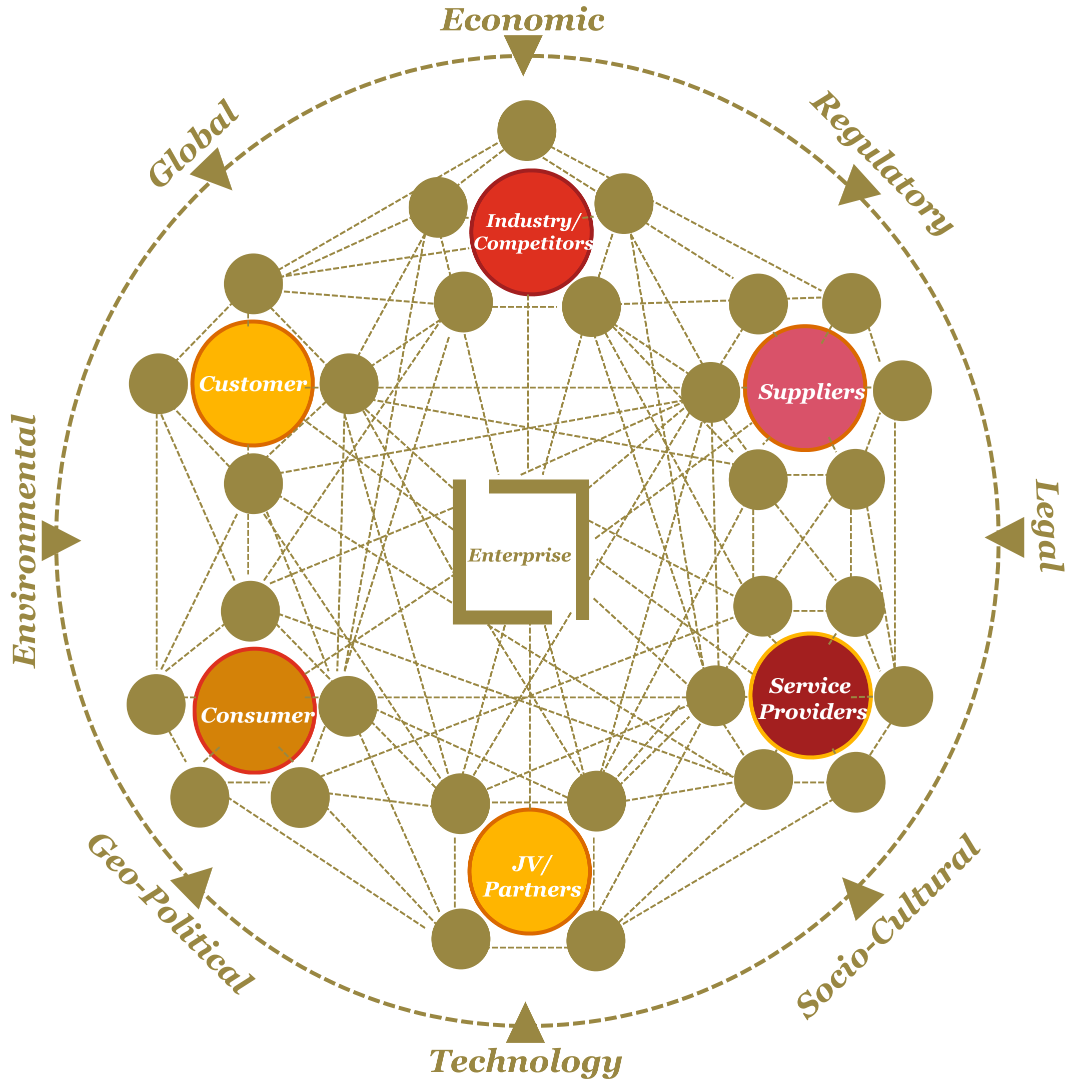
- Banks have to make huge investments in appropriate technologies.

- Regulators and law enforcement agents need to step up their game in the area of cybercrime prevention and detection, and in prosecuting proven criminals/perpetrators.

Thank you

Overview of the cyber threat landscape

The Global Business Ecosystem – the cyber challenge now extends beyond the enterprise



Traditional boundaries have shifted; companies operate in a dynamic environment that is increasingly interconnected, integrated, and interdependent.

- The ecosystem is **built around a model of open collaboration and trust**—the very attributes being exploited by an increasing number of global adversaries.
- Constant **information flow is the lifeblood of the business ecosystem**. Data is distributed and disbursed throughout the ecosystem, expanding the domain requiring protection.
- **Adversaries are actively targeting critical assets** throughout the ecosystem—significantly increasing the exposure and impact to businesses.

Years of underinvestment in security has impacted organizations' ability to adapt and respond to evolving, dynamic cyber risks.

Types of technology

Information Technology	Computing resources and connectivity for processing and managing data to support organizational functions and transactions
Operational Technology	Systems and related automation assets for the purpose of monitoring and controlling physical processes and events
Consumer Technology	Computing resources and connectivity to support external end-user focused products and services

“**Cybersecurity**” encompasses all three “**layers**”

Evolving business risks…

…impacting brand, competitive advantage, and shareholder value

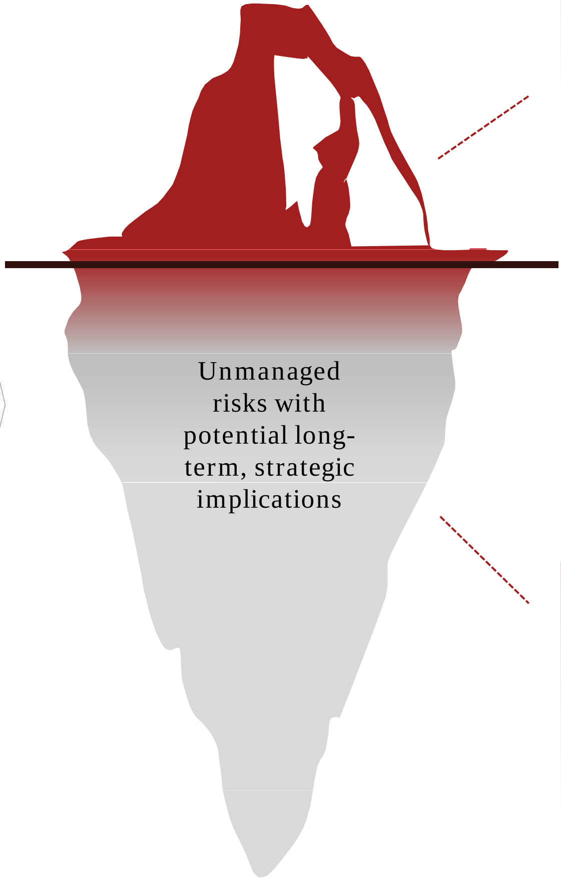
Highlights of activities impacting risk:

Advancements in and evolving use of technology *– adoption of cloud-enabled services; Internet of Things ("IoT") security implications; BYOD usage*

Value chain collaboration and information sharing *– persistent 'third party' integration; tiered partner access requirements; usage and storage of critical assets throughout ecosystem*

Operational fragility *– Real-time operations; product manufacturing; service delivery; customer experience*

Business objectives and initiatives *– M&A transactions; emerging market expansion; sensitive activities of interest to adversaries*


Unmanaged risks with potential long-term, strategic implications

Historical headlines have primarily been driven by compliance and disclosure requirements

However, the real impact is often not recognized, appreciated, or reported

Cybersecurity must be viewed as a strategic business imperative in order to protect brand, competitive advantage, and shareholder value

Cybercrime Landscape

The landscape is changing

Since 2009, the pace of economic collection and industrial espionage activities against major corporations and Government agencies is accelerating.

Objectives

- Economic espionage
- Industrial espionage
- Cyber-warfare
- Political statements
- Economic gain
- Recreation/Retaliation

Attack Techniques

- Outsourced hacking
- Custom exploits
- Custom malware
- Exploiting trusted relationships
- Targeted/Spear-phishing
- Hacker websites
- Social engineering
- Fly-by malware
- Mobile malware
- Requests for Information
- Solicitation of services
- Offers for joint ventures
- Foreign targeting of visitors overseas

Cyber threat actors

Adversary	Motives	Targets	Impact
Nation State	• Economic, political, and/or military advantage	• Trade secrets • Sensitive business information • Emerging technologies • Critical infrastructure	• Loss of competitive advantage • Disruption to critical infrastructure
Organized Crime	• Immediate financial gain • Collect information for future financial gains	• Financial / Payment Systems • Personally Identifiable Information • Payment Card Information • Protected Health Information	• Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence
Hacktivists	• Influence political and / or social change • Pressure business to change their practices	• Corporate secrets • Sensitive business information • Information related to key executives, employees, customers & business partners	• Disruption of business activities • Brand and reputation • Loss of consumer confidence
Insiders	• Personal advantage, monetary gain • Professional revenge • Patriotism	• Sales, deals, market strategies • Corporate secrets, IP, R&D • Business operations • Personnel information	• Loss of market share • Erosion of corporate confidence • National security impact

Nation States

What is at risk?

Information and communications technologies

Clean technologies

Military technologies

Advanced materials and manufacturing techniques

Healthcare, pharmaceuticals, and related technologies

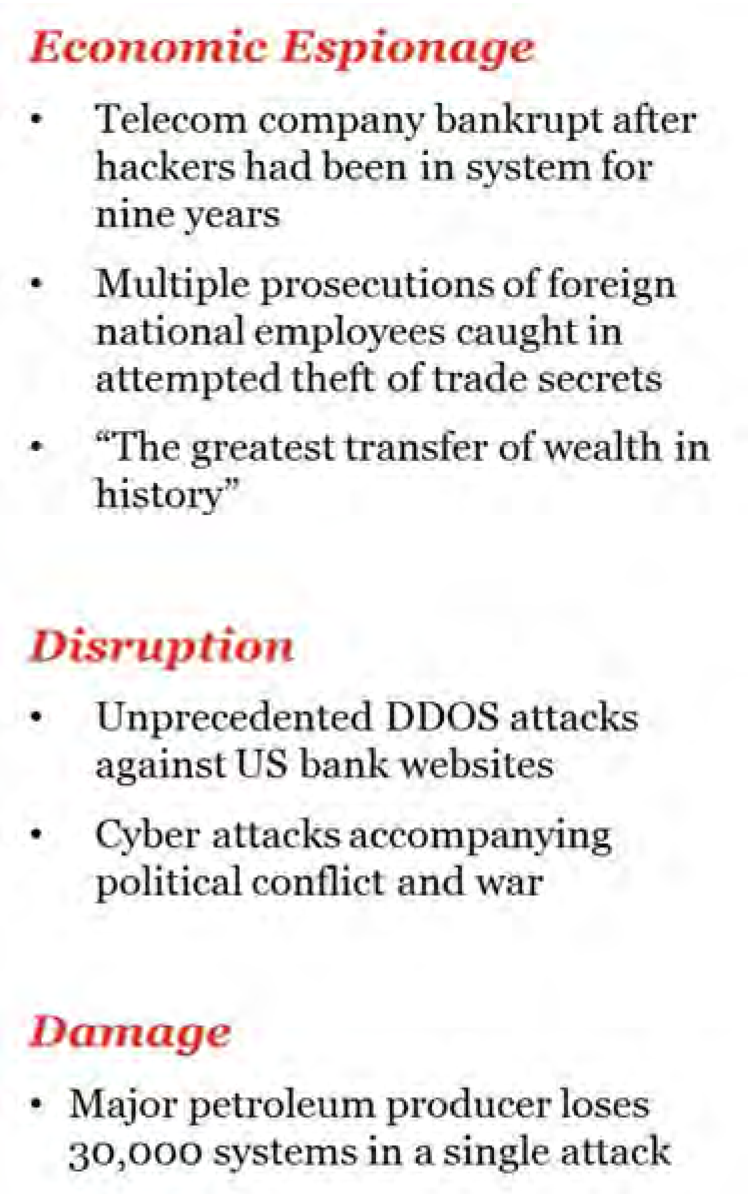
Agricultural technologies

Business deals information

Macroeconomic information

Energy and other natural resources information

Source: Office of the National Counterintelligence Executive, *Report to Congress on the Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011.*



Economic Espionage

- Telecom company bankrupt after hackers had been in system for nine years
- Multiple prosecutions of foreign national employees caught in attempted theft of trade secrets
- "The greatest transfer of wealth in history"

Disruption

- Unprecedented DDOS attacks against US bank websites
- Cyber attacks accompanying political conflict and war

Damage

- Major petroleum producer loses 30,000 systems in a single attack

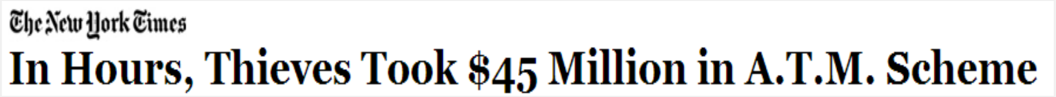
Organized Crime

Bank/Payment Card Fraud

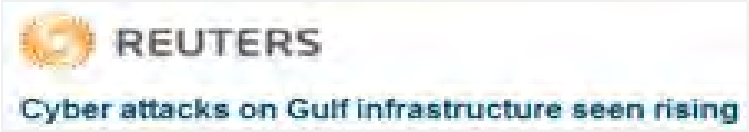
- An overseas card fraud gang hacked two financial institutions, gained account information, and cloned payment cards. Then they executed 36,000 transactions in 24 countries, withdrawing $40M in 10 hours.
- 2013 indictment of a gang who hacked a dozen financial institutions and retailers, stealing and reselling over 160M credit card numbers.

Identity Theft

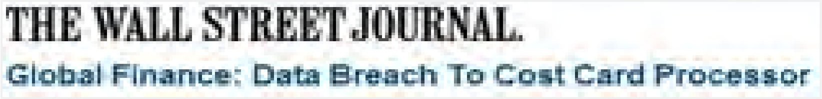
- Identity theft rings combine retail-based skimmers and illicit websites to steal consumer information.
- PII is typically exposed in bank breaches
- Regulatory response can often cost several times more than the theft.


The New York Times

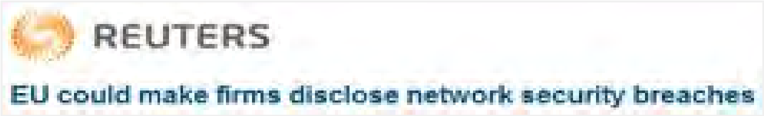
In Hours, Thieves Took $45 Million in A.T.M. Scheme


REUTERS

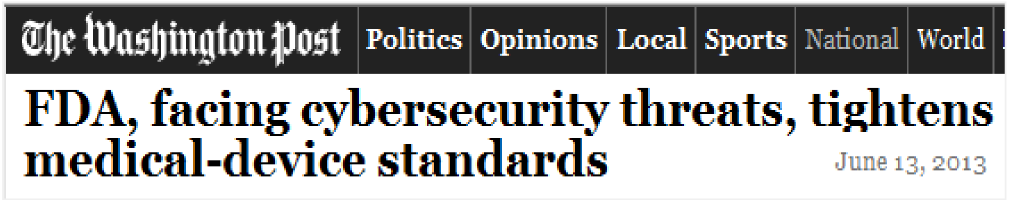
Cyber attacks on Gulf infrastructure seen rising


THE WALL STREET JOURNAL.

Global Finance: Data Breach To Cost Card Processor


REUTERS

EU could make firms disclose network security breaches



FDA, facing cybersecurity threats, tightens medical-device standards

June 13, 2013

Hacktivists

Collectives

- Anonymous/AnonOps, and LulzSec represent an increasing trend of global collectives.
- Targets include governments, financial institutions, lobbyists, terrorist groups, child pornography sites, religious organizations, and other hacker groups.
- Time Magazine named Anonymous one of the 100 most influential people in 2012.

Patriotic Hackers

- 2007 attacks on Estonia
- Attacks on supporters of Dalai Lama

Issue-focused groups

- Animal rights, environmentalism, anti-censorship

Tactics include:

- ***DDOS***
- ***Website defacing***
- ***Internet bullying***
- ***"Doxing"***

Insiders

Financially motivated

- On average, first incidents of fraud occur five years after hire
- FIs cite insiders as causing the majority of security incidents

Business or national security advantage

- David Yen Lee, convicted for using insider access to download 160 secret formulas for paints and coatings, with the intent to carry these secrets to a new job.
- Meng Hong convicted for downloading proprietary on organic light emitting diodes , intending to bring this information to a new job.

Disgruntled or Ideological

- Roger Duronio convicted of computer sabotage for inserting a logic bomb into employer's network, costing over $3M to remediate and days of enterprise-wide disruption.
- Edward Snowden

Some statistics on IT insider cases:

- 84% of IT insiders were motivated by revenge.
- 92% of all IT insiders attacked following a negative work-related event such as termination, dispute with a current or former employer, demotion, or transfer.
- 97% of all IT insiders came to the attention of supervisors or coworkers for concerning behavior prior to the attack.

> *"For the second year in a row, a greater number of respondents identified insider crimes (34%) as causing more damage to an organization than external attacks (31%)."*
>
> \- "Key Findings from the 2013 US State of Cybercrime Survey," PwC, June 2013

> *"The risk of from insider threats is not a technical problem, but a people-centric problem…what you have to do is take a multidisciplinary approach. One of the best resources your security program has is the collaboration of the HR Department."*
>
> \- Kate Randal, Insider Threat Analyst, FBI, 1 March 2013

What are the characteristics of the attackers our clients face?

1. ***Act on behalf of nation states***

   Many attacks originate from state-sponsored groups, given specific targets and objectives, who use information in replacement of traditional warfare weapons.

2. ***Use sophisticated and persistent methods of attack***

   Our breach analysis projects show that criminals perform considerable reconnaissance and adopt both high and low tech tactics to gain network access.

3. ***Target information for long term strategic gain***

   Threat actors are seeking valuable corporate intellectual property, blueprints , trade secrets, financial data, source code and PII.

4. ***Are global and multi-national***

   Many of the largest attacks originate from Eastern Europe, China, and Russia, with many groups having a multi-national component.

5. ***Are organized***

   Cybercrime syndicates (“hacktivists”), such as Anonymous, have thousands of members across the globe and coordinate attacks.

Nigerian Threat Landscape

Target Sectors	• Nigerian Think Tanks, Government Agencies • Nigerian Media • Various sectors of the Nigerian economy (Financial, Petroleum/oil and gas, Retail, power and energy, ICT, etc.) • High Profile Government websites • Much more..
Tactics	• Spear Phishing • Software Hijacking • Specific Nigerian Firewall and AV Targeting • Malware • DDoS • Colluding with insiders

Myth #1

Cyber threats are a technical issue managed locally

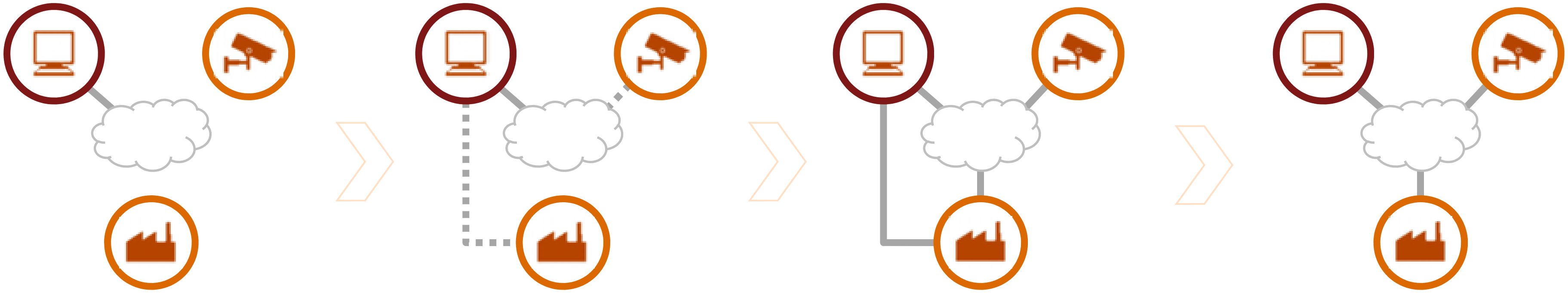
Reality: Threats are more than a local IT challenge – they are a global business challenge.

	Historical IT Security Perspectives	Today's Leading Cybersecurity Insights
Scope of the challenge	• Limited to your "four walls" and the extended enterprise	• Spans your interconnected global business ecosystem
Ownership and accountability	• IT led and operated	• Business-aligned and owned; CEO and board accountable
Adversaries' characteristics	• One-off and opportunistic; motivated by notoriety, technical challenge, and individual gain	• Organized, funded and targeted; motivated by economic, monetary and political gain
Information asset protection	• One-size-fits-all approach	• Prioritize and protect your "crown jewels"
Defense posture	• Protect the perimeter; respond if attacked	• Plan, monitor, and rapidly respond for when attacked
Security intelligence and information sharing	• Keep to yourself	• Public/private partnerships; collaboration with industry working groups

Myth #2

Threats to your data are limited to your networks

Technology convergence has increased opportunity, but businesses have not adapted to the new risks



1980s

- IT, OT and CT operate in different environments and on different platforms
- OT and CT are based on proprietary platforms
- Data is not shared between technologies
- **OT and CT face little to no cyber risk since they are not connected to a network**

1990s

- OT is networked to allow centralized operation
- CT remains in a separate environment
- **OT becomes vulnerable due to the connection, but is partially protected by the obscurity of proprietary solutions**

2000s

- OT connects to IT using standardized IT channels to reduce costs and increase compatibility
- Boundaries between IT and OT start to blur
- CT connects to IT through purpose built channels
- **OT is no longer protected by obscurity and CT is now vulnerable. Traditional IT security does not cover either**

2010+

- The technology underlying IT has become ubiquitous across OT and CT
- The combination of the three represents the integrated technology ecosystem
- **IT, OT, and CT are all vulnerable to cyber threats. Businesses must adapt their security model to include the full scope of technologies**

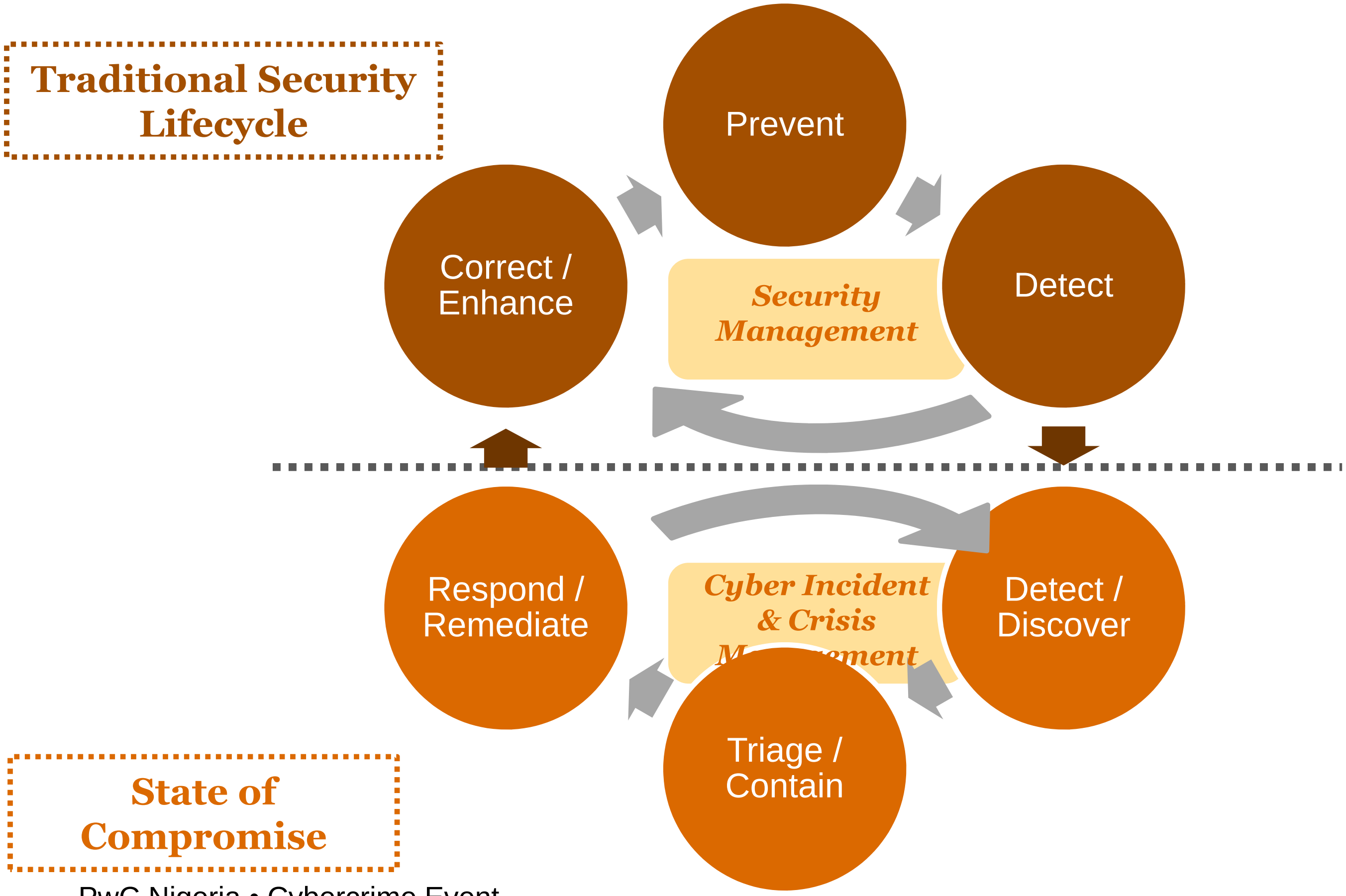
🖥	INFORMATION TECHNOLOGY
🏭	OPERATIONAL TECHNOLOGY
📹	CONSUMER TECHNOLOGY
☁	INTERNET
▪ ▪ ▪ ▪	PROPRIETARY CONNECTION
▬	IT PROTOCOL BASED CONNECTION

Myth #3

Cyber security is about keeping the hacker out

Reality: Not anymore. Evolution of IT as well as sophistication of the threat drives a need for anticipation and resilience, not just prevention.

Implication: **Effective cybersecurity includes understanding the threat, focused priority on critical data assets, and crisis response.**



Cyber Evolution:

A new holistic approach

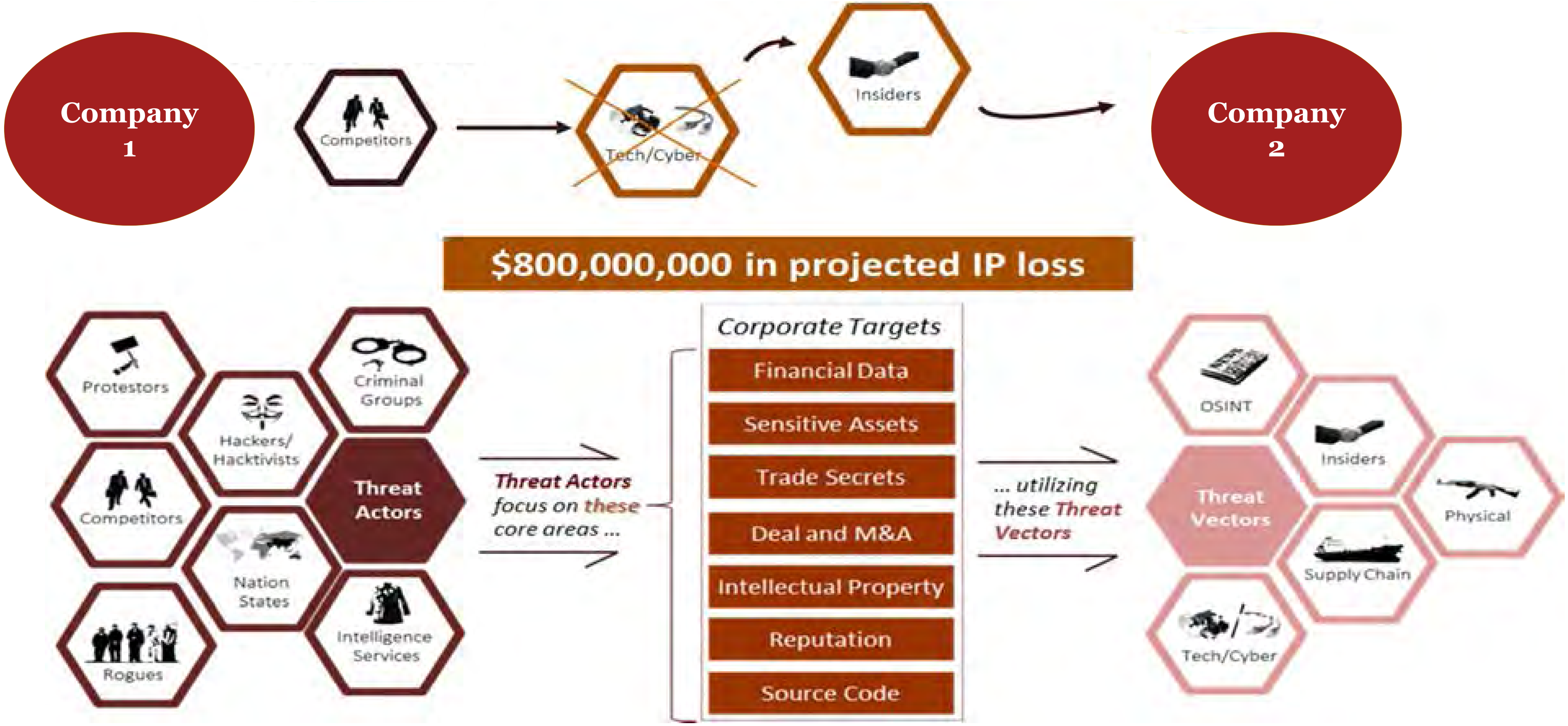
Increased volume, complexity and detection difficulty of attacks and the associated impact is driving enterprises to adopt a new approach to security.

Myth #4

Threat actors will stop attacking if you defend your IT networks

Reality: Probably not. Determined threat actors will use other other vectors if the cyber vector is too well defended or not available

Implication: **You need threat intelligence awareness about ALL the capabilities of threat actors, not just cyber**


Company 1

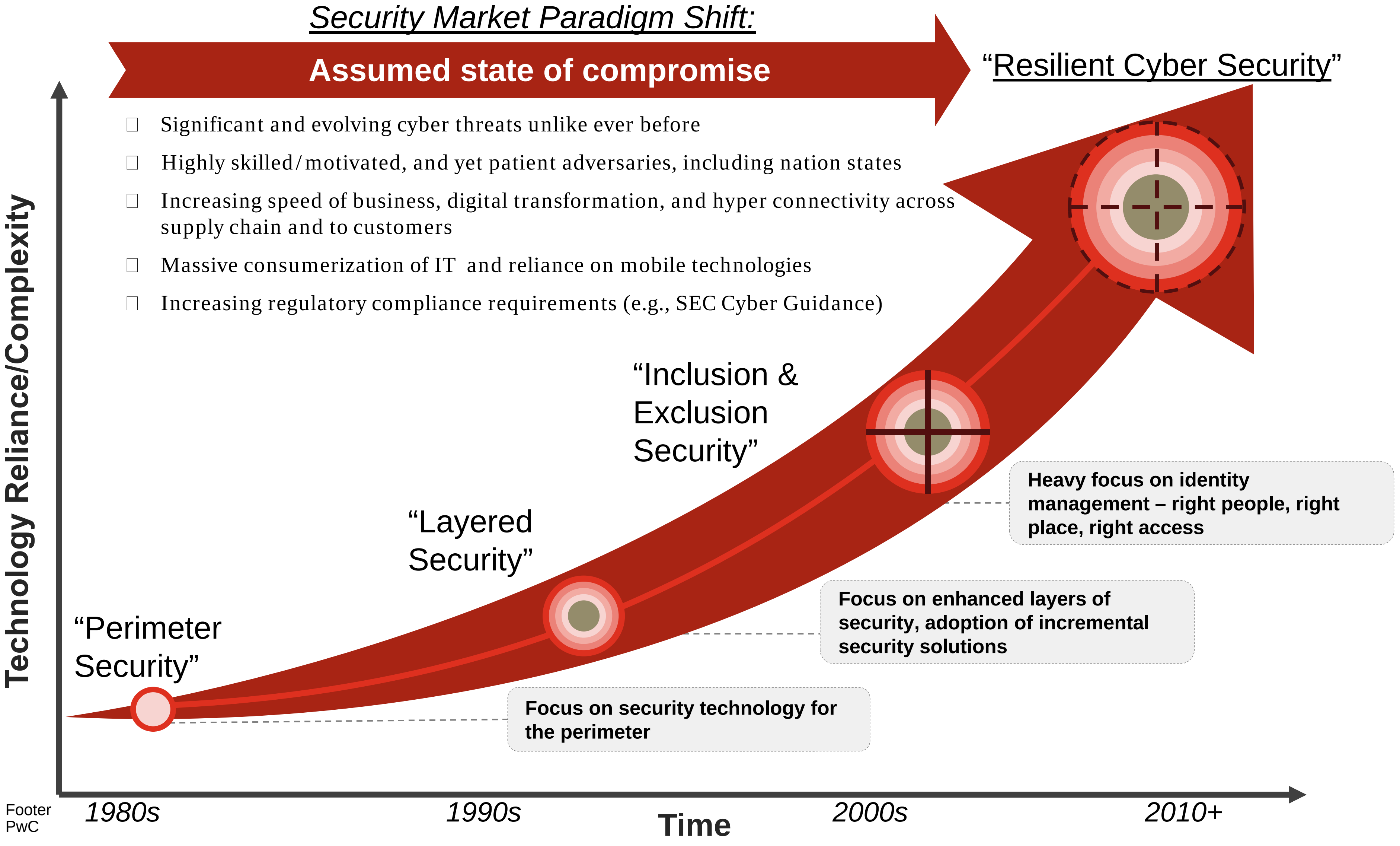
Company 2

Myth #5

You have not been hacked

Reality: Don’t bet on it. Advanced threats usually maintain remote access to target environments for 6-18 months before being detected.

Implication: **Effective cybersecurity assumes a state of compromise.**



Security Market Paradigm Shift:

Assumed state of compromise

“Resilient Cyber Security”

- Significant and evolving cyber threats unlike ever before
- Highly skilled/motivated, and yet patient adversaries, including nation states
- Increasing speed of business, digital transformation, and hyper connectivity across supply chain and to customers
- Massive consumerization of IT and reliance on mobile technologies
- Increasing regulatory compliance requirements (e.g., SEC Cyber Guidance)

“Inclusion & Exclusion Security”

Heavy focus on identity management – right people, right place, right access

“Layered Security”

Focus on enhanced layers of security, adoption of incremental security solutions

“Perimeter Security”

Focus on security technology for the perimeter

Break until 11:15 AM

Interactive Session - Through the Eyes of an Attacker

Understanding Threat Actors: Your Turn to Attack

Now you have the chance to change perspectives

Your companies are constantly targeted by threat actors. These actors range from opportunistic groups seeking to create short-term disturbances to organized, strategic actors with specific objectives, extensive resources, and long term goals in mind.

Today, you will be the attacker.

Your decisions will drive the outcome – **success!** (plunder and profit), or **failure** (arrest, indictment or even a counterattack).

Your Mission

Identify the intentions of a malicious attacker, find vulnerable target, choose an appropriate method of attack, and attempt a successful breach.

Which attacker will you be?

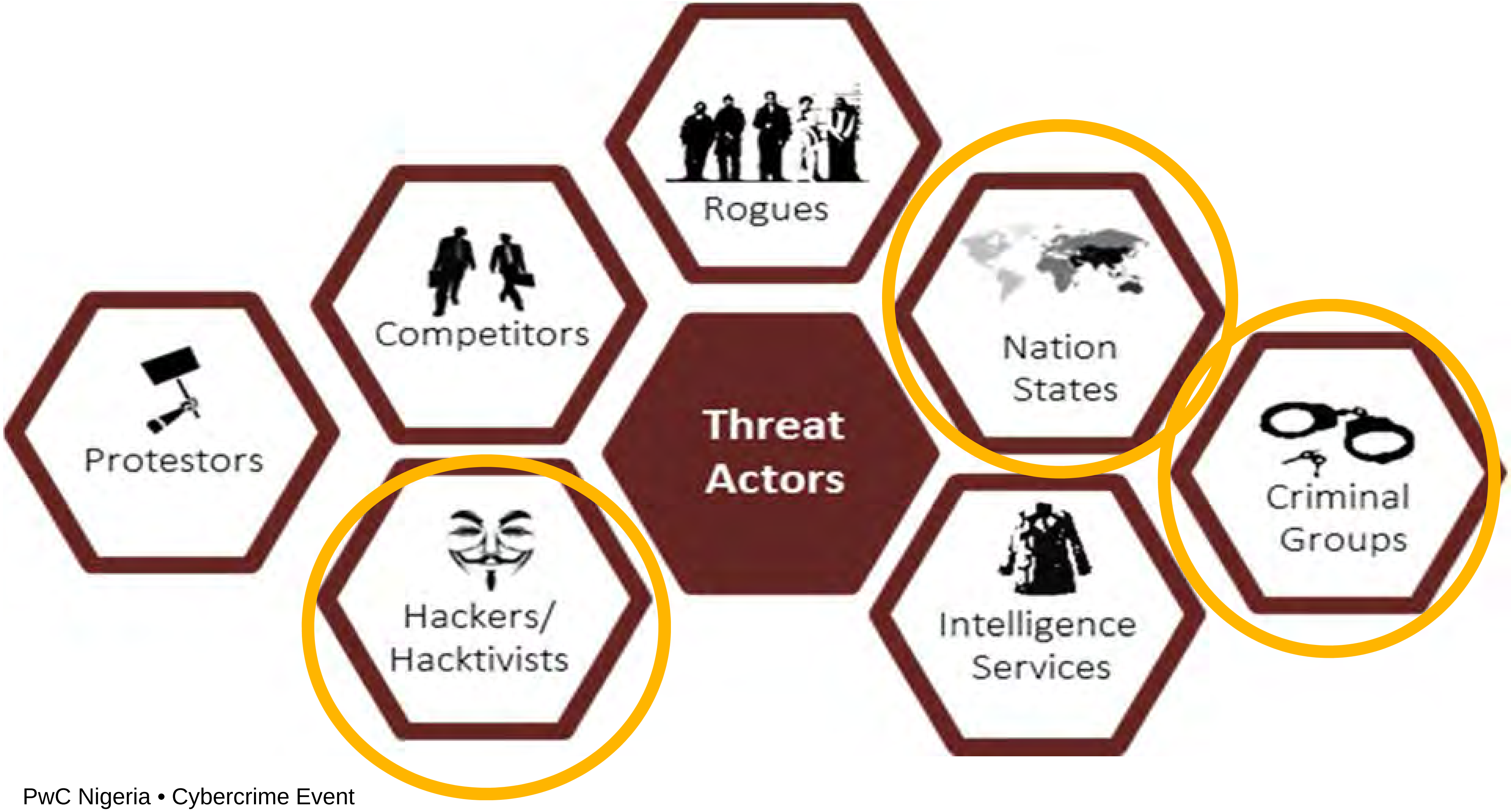
Who will you target?

What is of greatest value?

How will you attack?

Choose Your Threat Actor

Who are you?



Threat Actor Trends

Organized crime groups have advanced from small-scale monetary theft to large-scale multi-country simultaneous heists.

A growing number of nation states are getting into the cyberattack game.

Hacktivists are working with sympathizers within organizations to gain better access.

[1] *The Global State of Information Security Survey® 2014, Retail and Consumer Key Findings, PwC, September 2013*

Threat Actor 1: Organized Crime
Nasha Veshch

- Tactically exploit targets for financial gain
- Focuses on financial industry for access to payment cards, credentials, and bank accounts
- Also seeks IP, industrial secrets, and marketing plans to sell
- Short-term goals, willing to abandon targets if difficulties arise
- Business partners include drug and human traffickers, arms dealers, terrorist organizations, and nation-state pariahs
- Uses common high-tech tools including automated exploit kits

Threat Actor 2: Hacktivists

Guy Wulfe

- Embarrasses companies and their customers by destroying brand reputation, exposing private or proprietary information
- Seeks to publish personal information and internal organization data as punishment for greed – or just for Lulz
- Hacking feats are well documented and continually recruiting hackers with expert technical capabilities
- Responsible for numerous DDoS attacks on major corporations; published career-ending compromising pictures of a pro-business politician.

Threat Actor 3: Nation State

APT-24x7x365

- Cyber military unit of a large nation looking to further national interests
- Seeks military info, economic plans, trade secrets, or technical resources
- Invests extensive time and effort in strategic endgame; targets various organizations for separate parts of a single strategy
- Deep pockets, cutting-edge technology, and extensive talent pool
- Not motivated by immediate financial gain
- Will stay hidden until their mission is accomplished; will fervently protect investments of resources and time

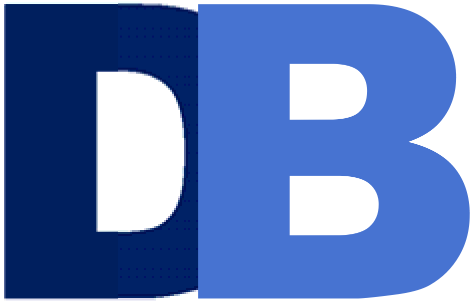
Which attacker will you portray?

1

2

3

You know who you are.
Who will you attack?



Industry Trends

Hackers are the likely perpetrators in 36% of security incidents in the financial industry

In the retail and consumer industry, rates of compromised employee and customer records increased by more than 50% over last year

Current employees are cited in 43% of security incidents in healthcare companies

Target Company 1: International Retailer *Gimbelles*

- International retail chain with stores and manufacturing in Southeast Asia
- Processes millions of transactions at stores and online; expanding online payment options
- Heavily promotes its popular store loyalty program
- Actively increasing their online presence, using social media to interact with consumers
- Beginning to transfer more of its processes to the cloud, including storage of employee and customer records

Target Company 2:

International Medical Device Manufacturer

HeartTrax

- Produces cutting-edge medical equipment used around the globe
- Invests heavily in new product development
- Devices are wireless and linked through an internal network
- Offices and suppliers are linked over the web
- Has recently begun an insider threat management program
- Some devices use rare or radioactive materials; some tools used in manufacturing the equipment are dual-use technologies

Target Company 3:
Global Finance Institution
DankeBank

- Global banking institution offering wide range of financial products
- Game-changing emerging market M&A on the horizon
- Expanding online presence and products; switching to cloud computing
- Employs sophisticated high-frequency trading systems
- Allows employees to BYOD

What business assets are of greatest value?

	Vulnerability		
	Regulated Data Elements	Crown Jewel	Greatest Exposure
Gimbelles	PCI, PII	Customer Loyalty Data	Historic Lack of Focus on Security
HeartTrax	PHI, PII	Medical Technology R&D	Wireless Med Devices
DankeBank	PII, PCI	Trading Algorithms	Upcoming M&A

*Risk = Probability[(Vulnerability * Likelihood)/Controls]*

Who will you attack?

1. Gimbelles

2. HeartTrax

3. DankeBank

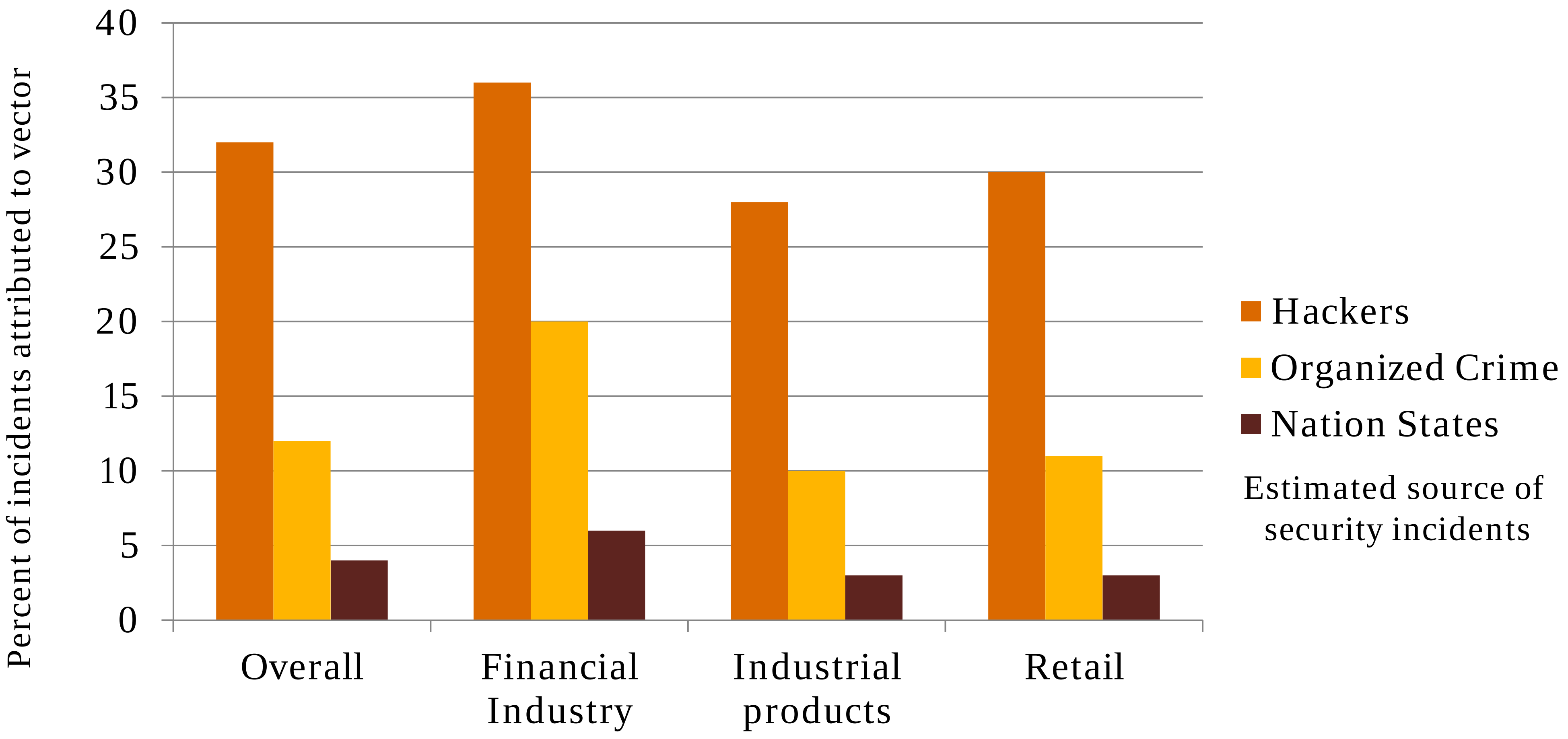
You know who you are.
You know who and what you will be targeting.

How will you attack?

1. **Exploit Technical Vulnerabilities**
2. **Target Executive Communications**
3. **Engage an insider threat**

How do you line up? Trends we're seeing:

The 2014 PwC The Global State of Information Security Survey shows trends of threat to specific industries:



Attack Option 1:

Exploit Technical Vulnerabilities

- You will use high-level technical skills to exploit system vulnerabilities.

- Companies that lack up-to-date software patches or that lack consistent cyber security practices are the most susceptible

- System access will allow you to steal credentials, allowing you to build in future access capabilities into the system

Attack Option 2:

Target Executive Communications

- You will target the high level information available in executive communications

- Each of the many devices used by executives presents a node of possible attack

- You will use social media and online information to identify influential people with necessary access

- You hope to gain information on upcoming business deals or embarrassing personal information

Attack Option 3:

Engage an Insider

- You will target individuals with access that can be used to illicitly access desired information
- You may approach an IT employee with debt and financial responsibilities or consider bribing a security guard or cleaning staff to steal a laptop to insert a thumb drive into a server to execute malware
- You have begun to identify possible insiders through their public social media denouncing the company

Human and Technical vulnerabilities are equally valuable targets

	Exploit Technical Vulnerabilities	*Target Executive Communications*	*Engage an Insider*
Gimbelles	PCI	Business Strategies PII	Customer Loyalty Data
HeartTrax	Access to Wireless Med Devices PHI	Business Strategies PII	Medical Technology R&D
DankeBank	Financial Account Information PCI	Upcoming M&A PII	Trading Algorithms

Human Vulnerabilities

Technical Vulnerabilities

How will you attack?

1. **Exploit Technical Vulnerabilities**

2. **Target Executive Communications**

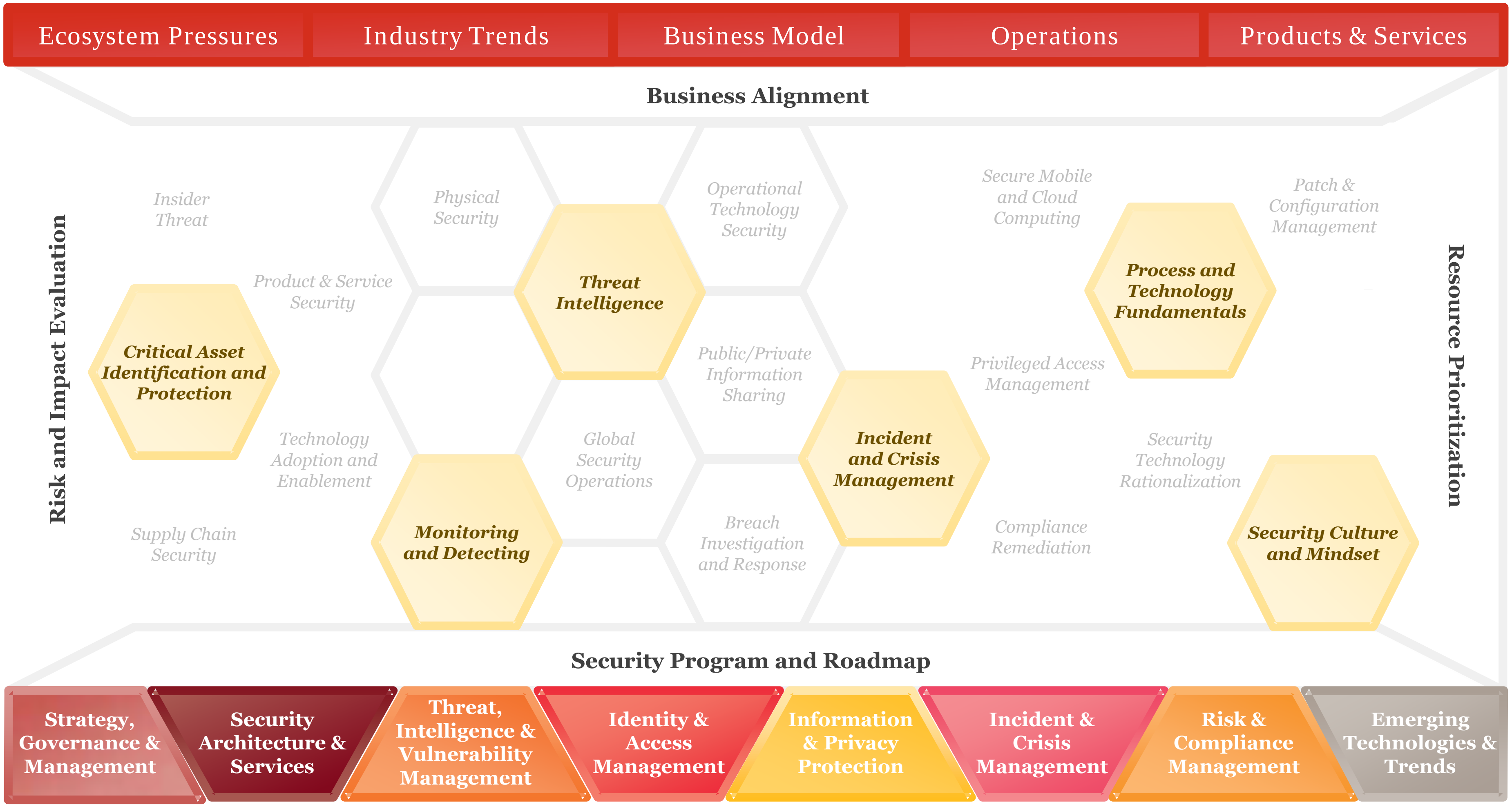
3. **Engage an Insider Threat**

In our view, most of these cybersecurity challenges can be addressed internally.

"The majority of attacks (roughly 80%) rely on exploits that companies can readily defend against, if they focus their attention on fundamental cybersecurity education, properly maintained IT infrastructure, and effective monitoring."

- 2013 US State of Cybercrime Survey

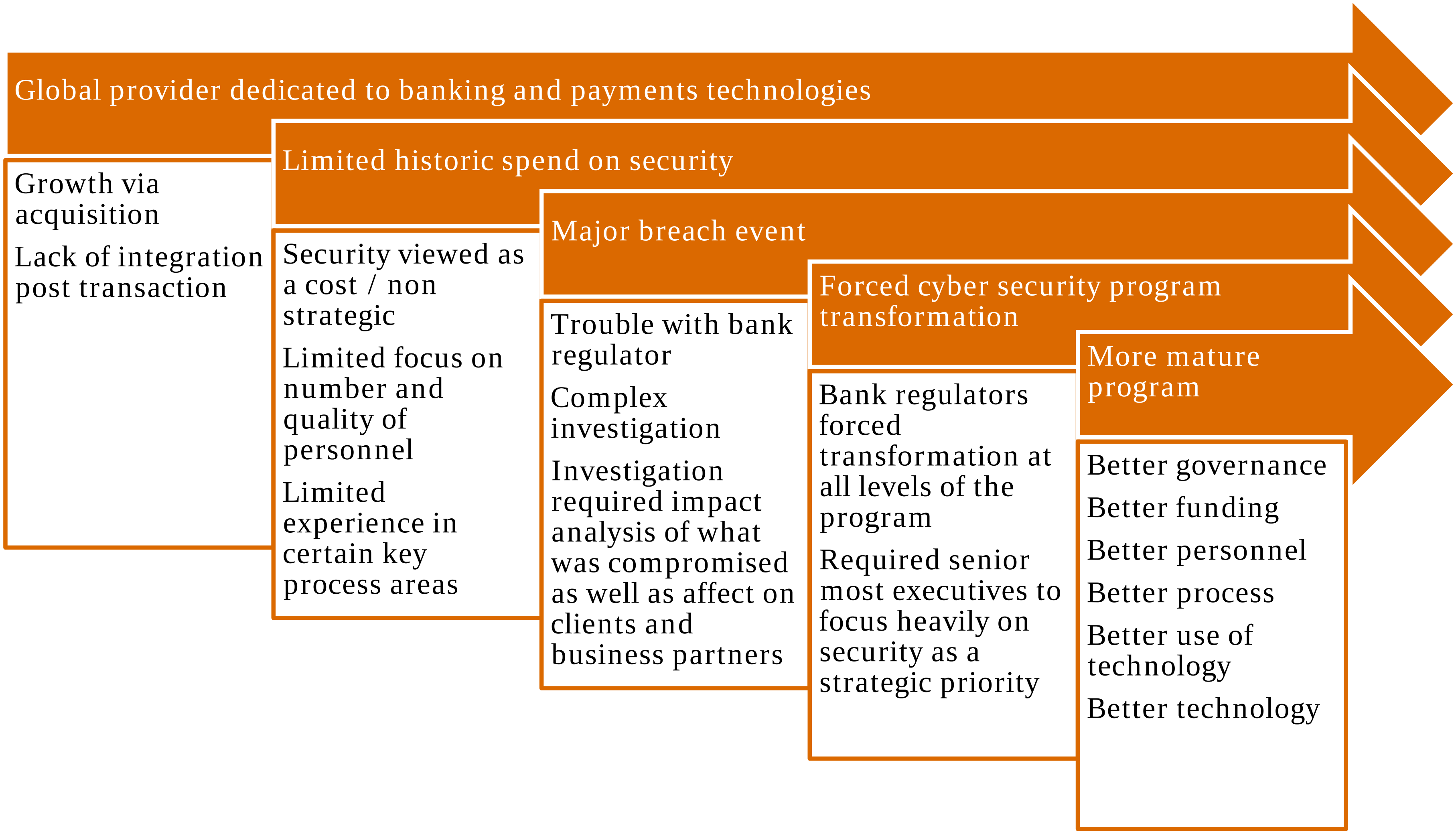
Fundamental Investment Areas


Ecosystem Pressures
Industry Trends
Business Model
Operations
Products & Services
Business Alignment
Risk and Impact Evaluation
Resource Prioritization
Insider Threat
Physical Security
Operational Technology Security
Secure Mobile and Cloud Computing
Patch & Configuration Management
Threat Intelligence
Process and Technology Fundamentals
Product & Service Security
Critical Asset Identification and Protection
Public/Private Information Sharing
Privileged Access Management
Technology Adoption and Enablement
Global Security Operations
Incident and Crisis Management
Security Technology Rationalization
Supply Chain Security
Monitoring and Detecting
Breach Investigation and Response
Compliance Remediation
Security Culture and Mindset
Security Program and Roadmap
Strategy, Governance & Management
Security Architecture & Services
Threat, Intelligence & Vulnerability Management
Identity & Access Management
Information & Privacy Protection
Incident & Crisis Management
Risk & Compliance Management
Emerging Technologies & Trends

Case Study

A major financial services company suffered a significant network intrusion which resulted in the theft of millions of dollars and the compromise of certain client and company confidential data.

Client Situation



Global provider dedicated to banking and payments technologies

Growth via acquisition

Lack of integration post transaction

Limited historic spend on security

Security viewed as a cost / non strategic

Limited focus on number and quality of personnel

Limited experience in certain key process areas

Major breach event

Trouble with bank regulator

Complex investigation

Investigation required impact analysis of what was compromised as well as affect on clients and business partners

Forced cyber security program transformation

Bank regulators forced transformation at all levels of the program

Required senior most executives to focus heavily on security as a strategic priority

More mature program

Better governance

Better funding

Better personnel

Better process

Better use of technology

Better technology

Cashout Operation related to Pre-Paid Debit Cards

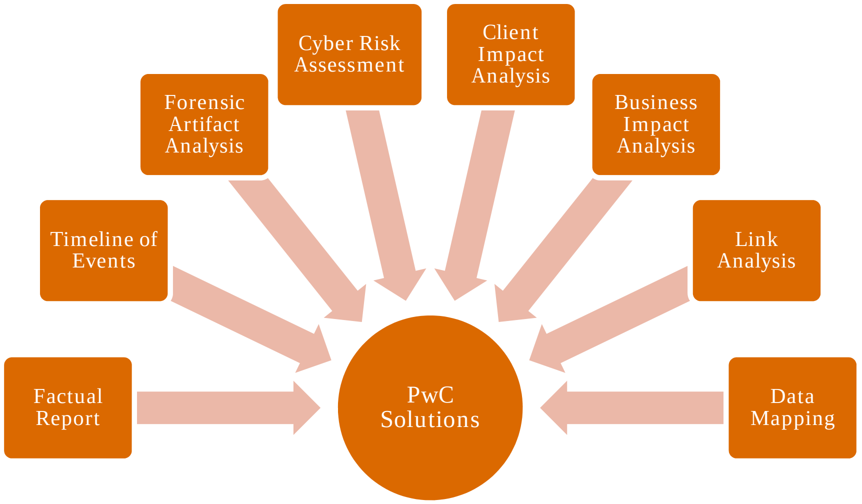
Client issue

A major financial services company suffered a significant network intrusion which resulted in the theft of millions of dollars and the compromise of certain client and company confidential data. The company's network was accessed by exploiting a known vulnerability in an Internet facing system which resulted in the intruders gaining access to the internal network of the company, including certain administrator credentials. The setting in which the network intrusion occurred was marked by a significant corporate governance deficiency. The company sought to verify findings from previous investigators and based on PwC's validation and new findings, address concerns raised by government regulators.

PwC actions

PwC, along with external counsel, were engaged by the Company to develop a factual report outlining the nature, scope, extent and timeline of events related to the network intrusion, including a forensic artifact analysis, a cyber risk assessment and a client impact assessment. As a result, PwC deployed a large, multi capable team made up of Forensic, Cyber Security and Washington Federal resources that:

- Developed a governance and project structure to manage a very complex, multi stakeholder investigation.
- Performed a risk analysis of compromised systems that prioritized systems to be imaged; imaged more than 140 systems.
- Analyzed numerous forensic images amounting to over 120TB of data and other technical information to develop a factual understanding of the intrusion, including a timeline of the events leading up to and after the intrusion.
- Extracted and loaded 435 million forensic artifacts into a link analysis tool.
- Conducted informational and technical interviews with over 200 key custodians and business and technical application owners.
- Analyzed email data through a third party review platform.
- Reviewed individual contents of files for clients referenced, sensitive data elements, intellectual property contained, and cyber risks associated with each file.
- Determined the business, cyber and regulatory impact of the data that was exposed .
- Developed a comprehensive factual report confirming (or disputing) previous investigation findings and provided new facts for Company consideration.



Results of Investigation

Today the Company and its management appreciate the extent of, and the risks associated with, the Network Intrusion, which has enabled senior management to prioritize remediation activities to effectively strengthen the Company's security and its evidence preservation policies and processes, respond to regulators' concerns, and protect the Company's reputation. PwC's comprehensive factual report and investigation assisted the company in the following areas:

Government Regulators

- Facts to respond to inquiries
- Improve communications and relationships

Impacted Clients

- Creation of communication plan
- Creation of client notification packages

Cyber Security

- Identified risks
- Assisted with remediation of cyber risks

Company's Technical Infrastructure

- Provided guidance to secure and enhance
- Created a program to meet and exceed industry benchmarks

Incident Response

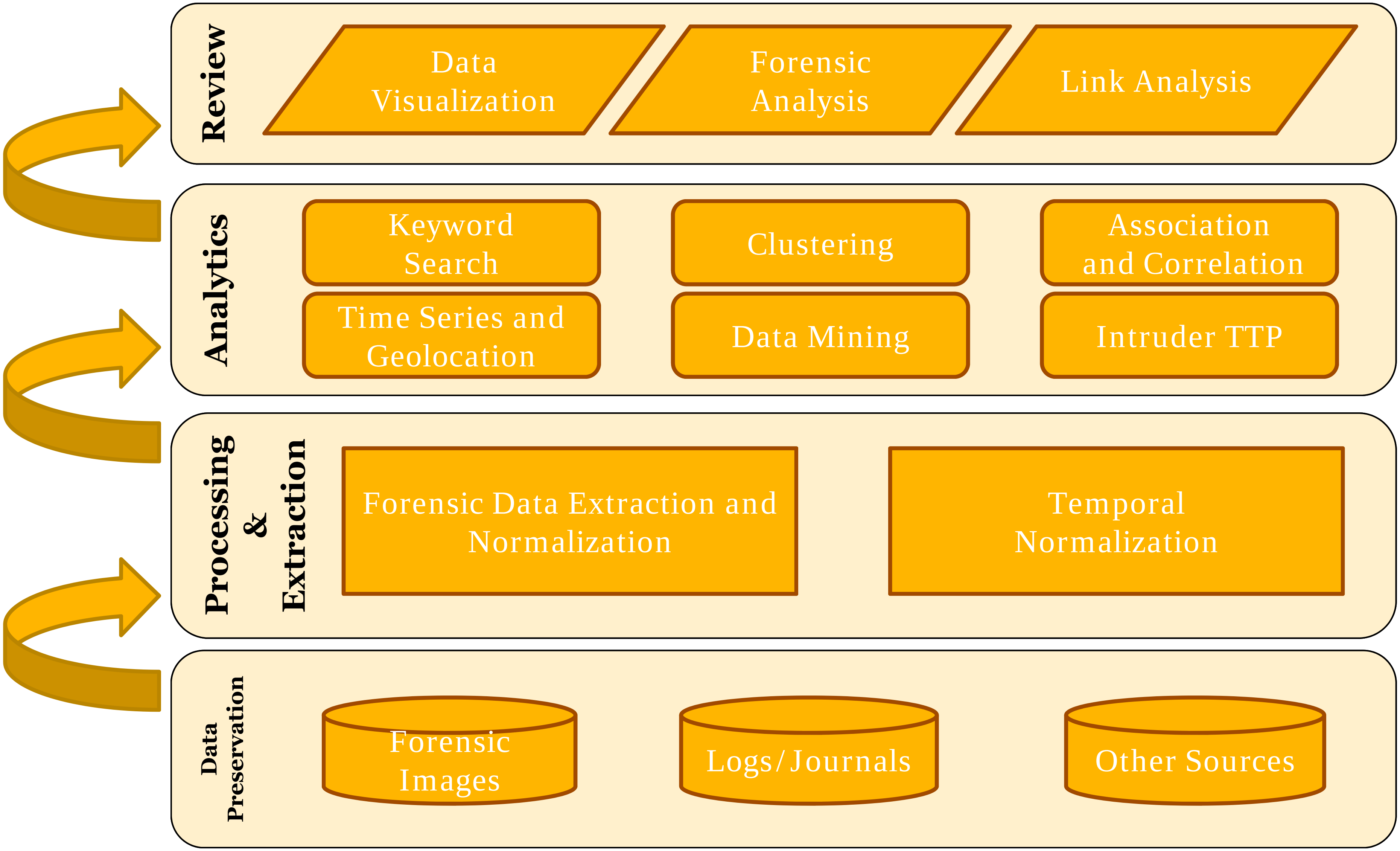
- Improved the Company's process

Inputs the System

This platform took the following data as inputs:

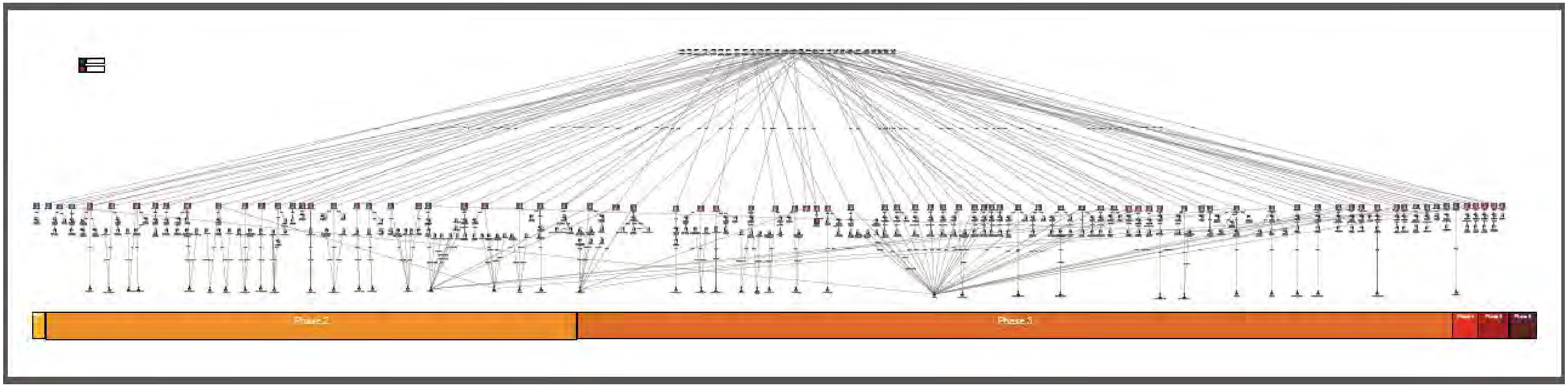
- Forensic images collected during the Incident and later review
- Associated network, security and host logs
- Emails
- Business/organizational information
- Intelligence developed by PwC over the history of breach responses

PwC's Rapid Analytics and Visualization in Enterprise Networks (RAVEN) Architecture

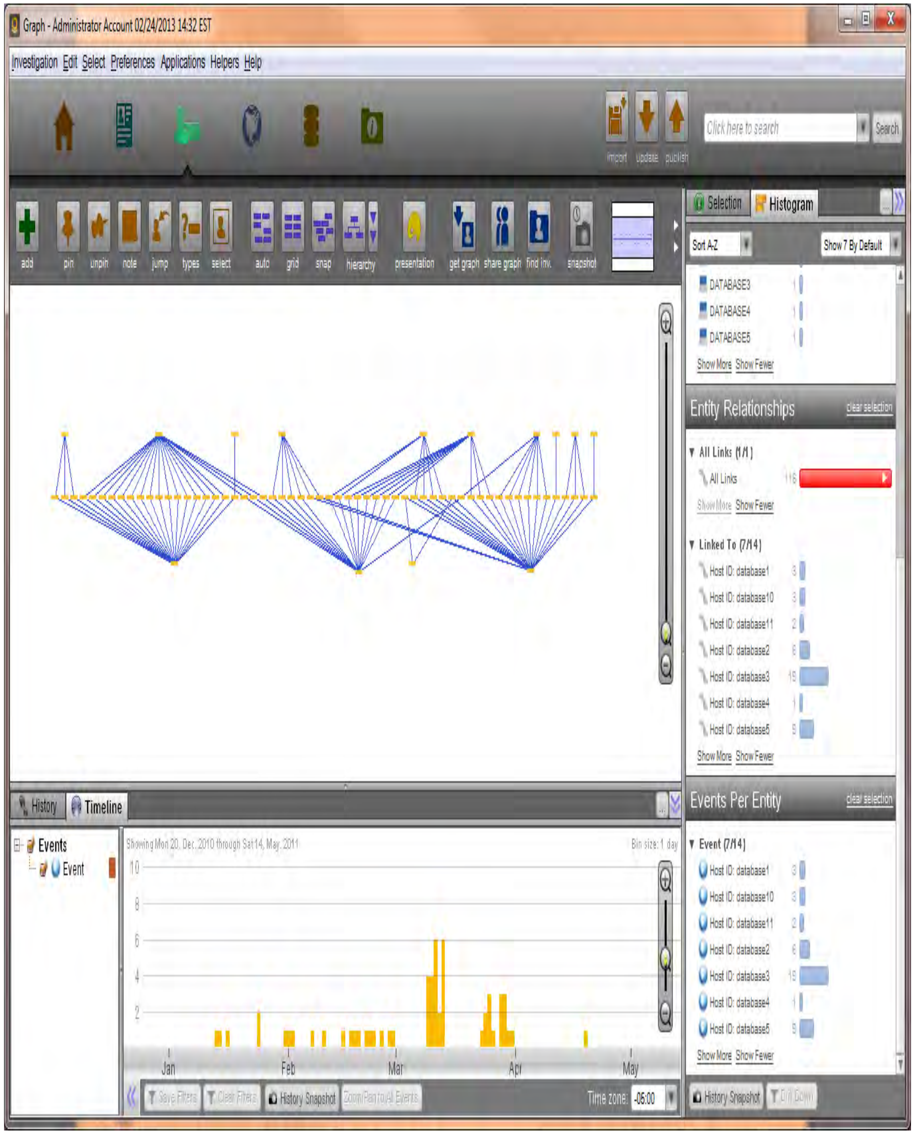


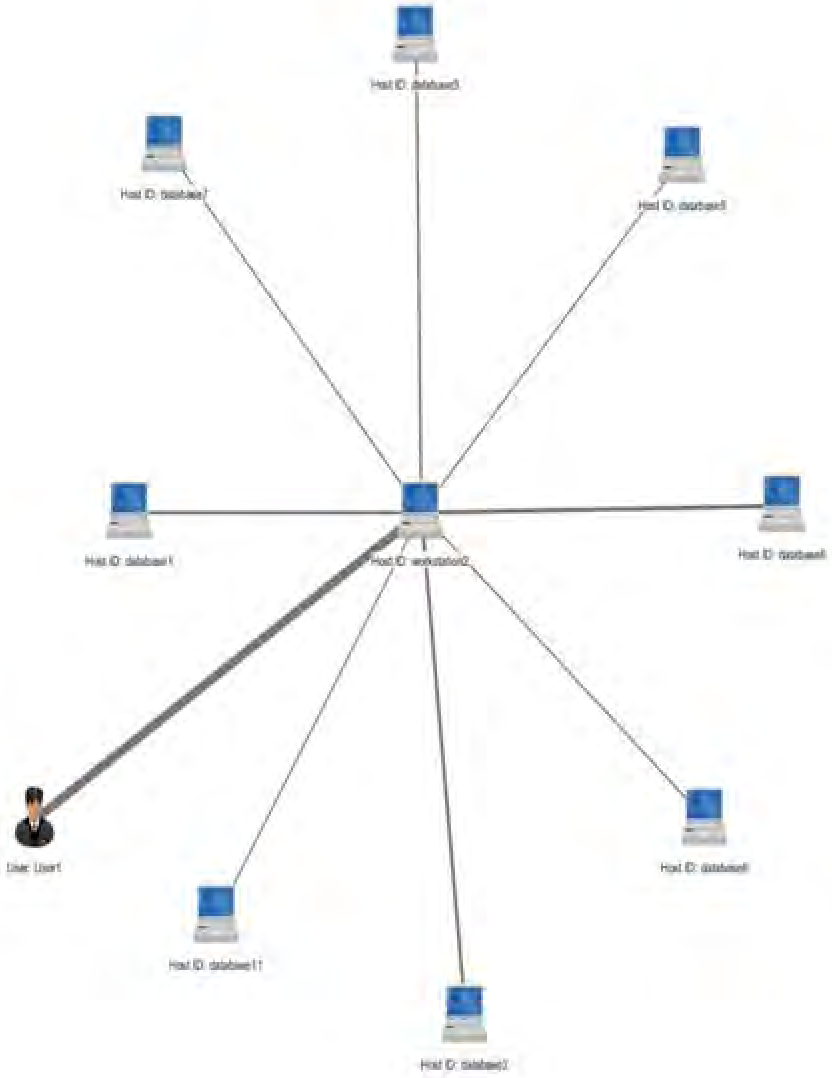
Outputs

- An overall incident visualization depicting systems affected
- Day-by-day visual breakdowns of significant Intruder activity
- Reports of how specific customers were affected
- Reports of how specific systems were affected

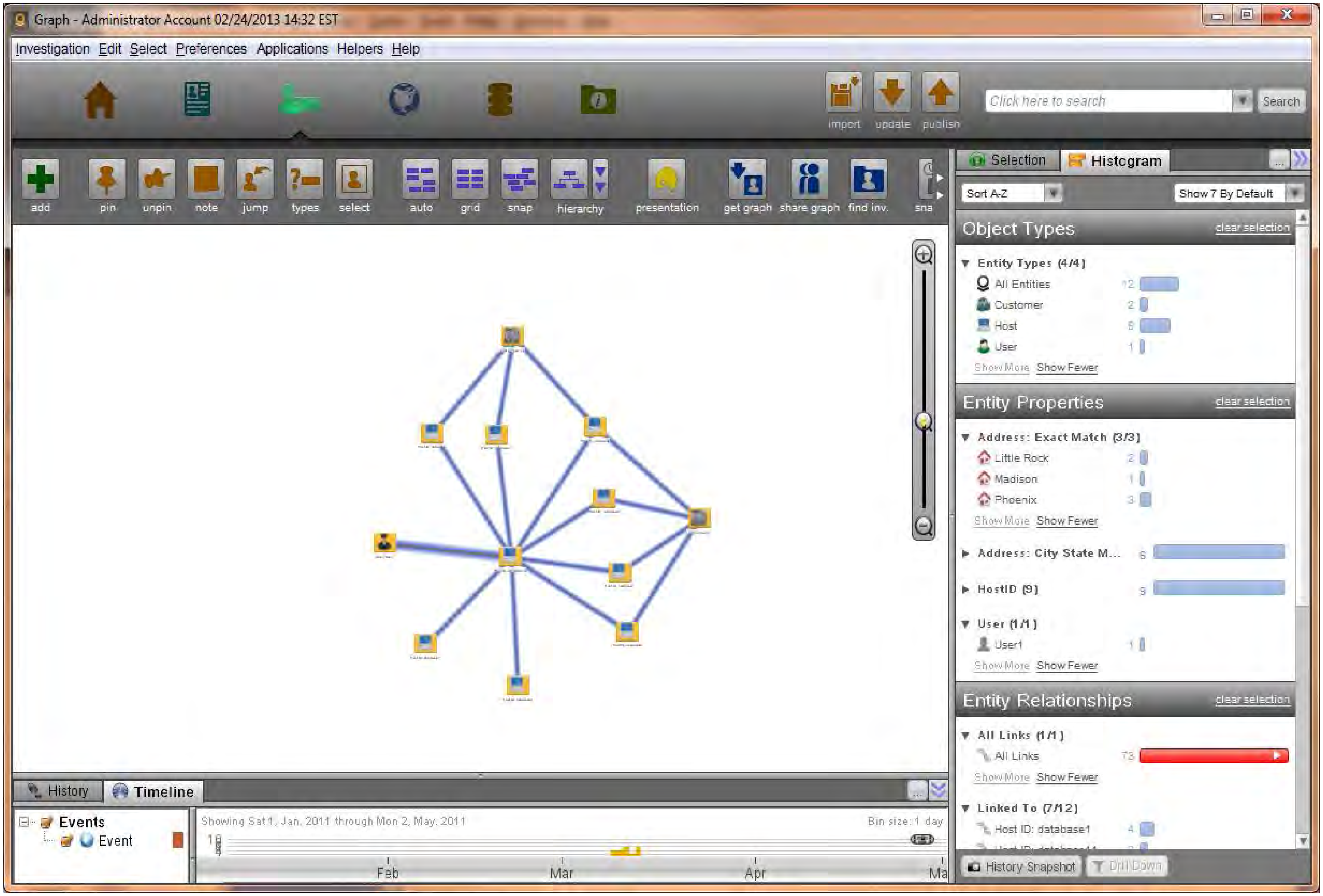


Viewing the Structure





What clients data are on systems in question?



Showing Sat 1, Jan, 2011 through Mon 2, May, 2011

Bin size: 1 day

Sort A-Z

Show 7 By Default

Object Types — clear selection

▼ Entity Types (4/4)

All Entities	12
Customer	2
Host	9
User	1

Show More Show Fewer

Entity Properties — clear selection

▼ Address: Exact Match (3/3)

Little Rock	2
Madison	1
Phoenix	3

Show More Show Fewer

▶ Address: City State M...	6
▶ HostID (9)	9

▼ User (1/1)

User1	1

Show More Show Fewer

Entity Relationships — clear selection

▼ All Links (1/1)

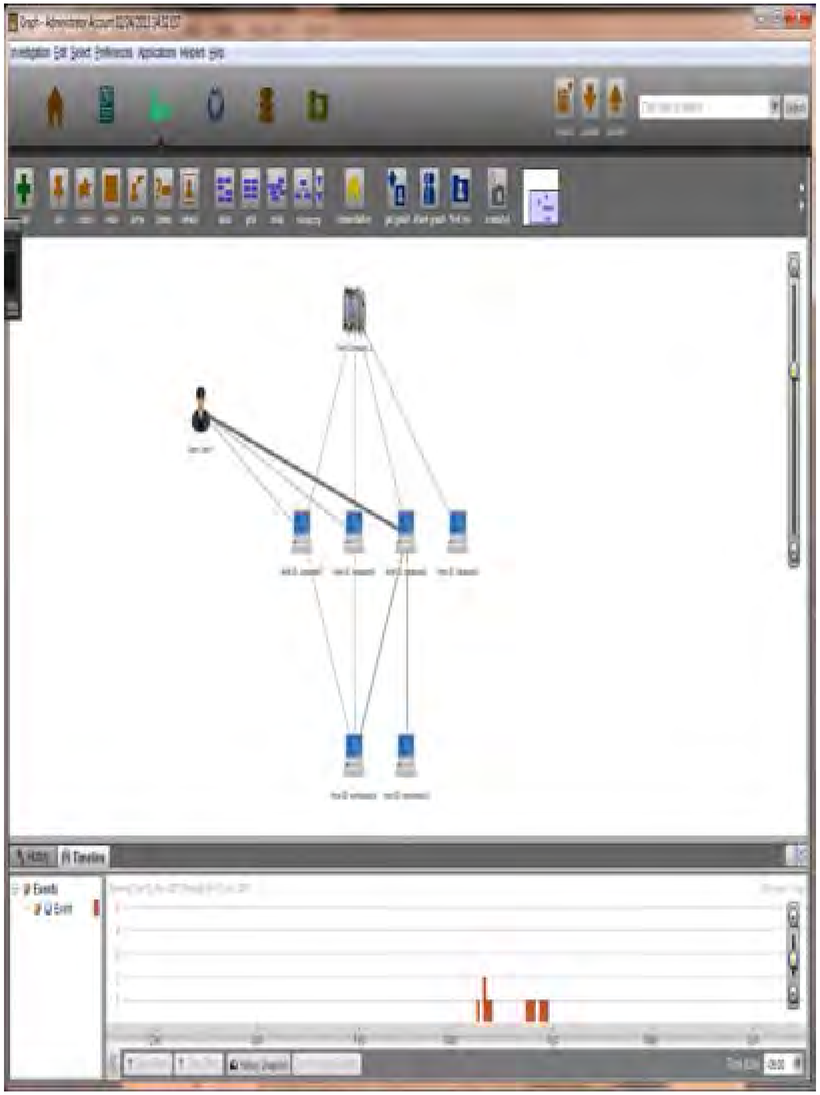
All Links	73

Show More Show Fewer

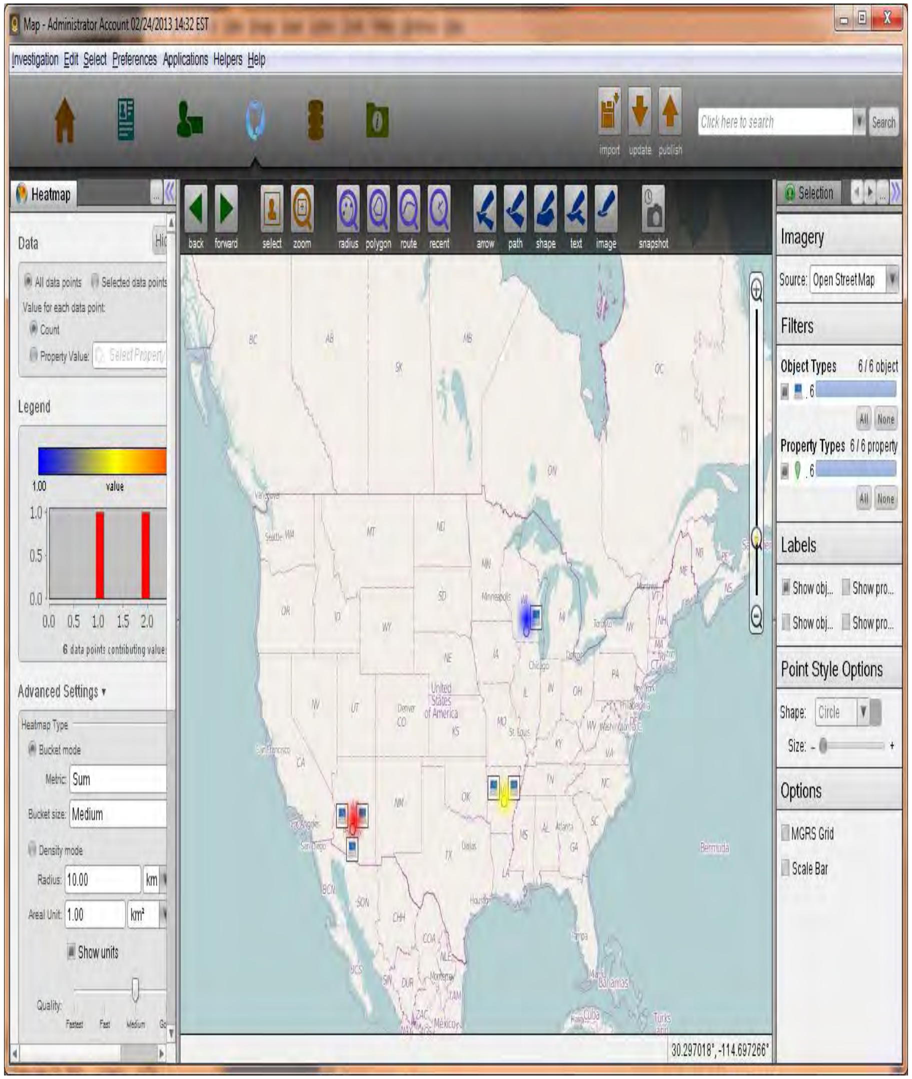
▼ Linked To (7/12)

Host ID: database1	4

How was customer X affected?


Investigation Edit Select Preferences Applications Helpers Help
History
Timeline
Events
Event

Where was customer X located?



● All data points ○ Selected data points

Value for each data point:

● Count

○ Property Value: Select Property

6 data points contributing value

Heatmap Type

● Bucket mode

Metric: Sum

Bucket size: Medium

○ Density mode

Radius: 10.00 km

Areal Unit: 1.00 km²

☒ Show units

Quality: Fastest Fast Medium

Source: Open StreetMap

Object Types 6 / 6 object

Property Types 6 / 6 property

☒ Show obj... □ Show pro...

□ Show obj... □ Show pro...

Shape: Circle

Size: - +

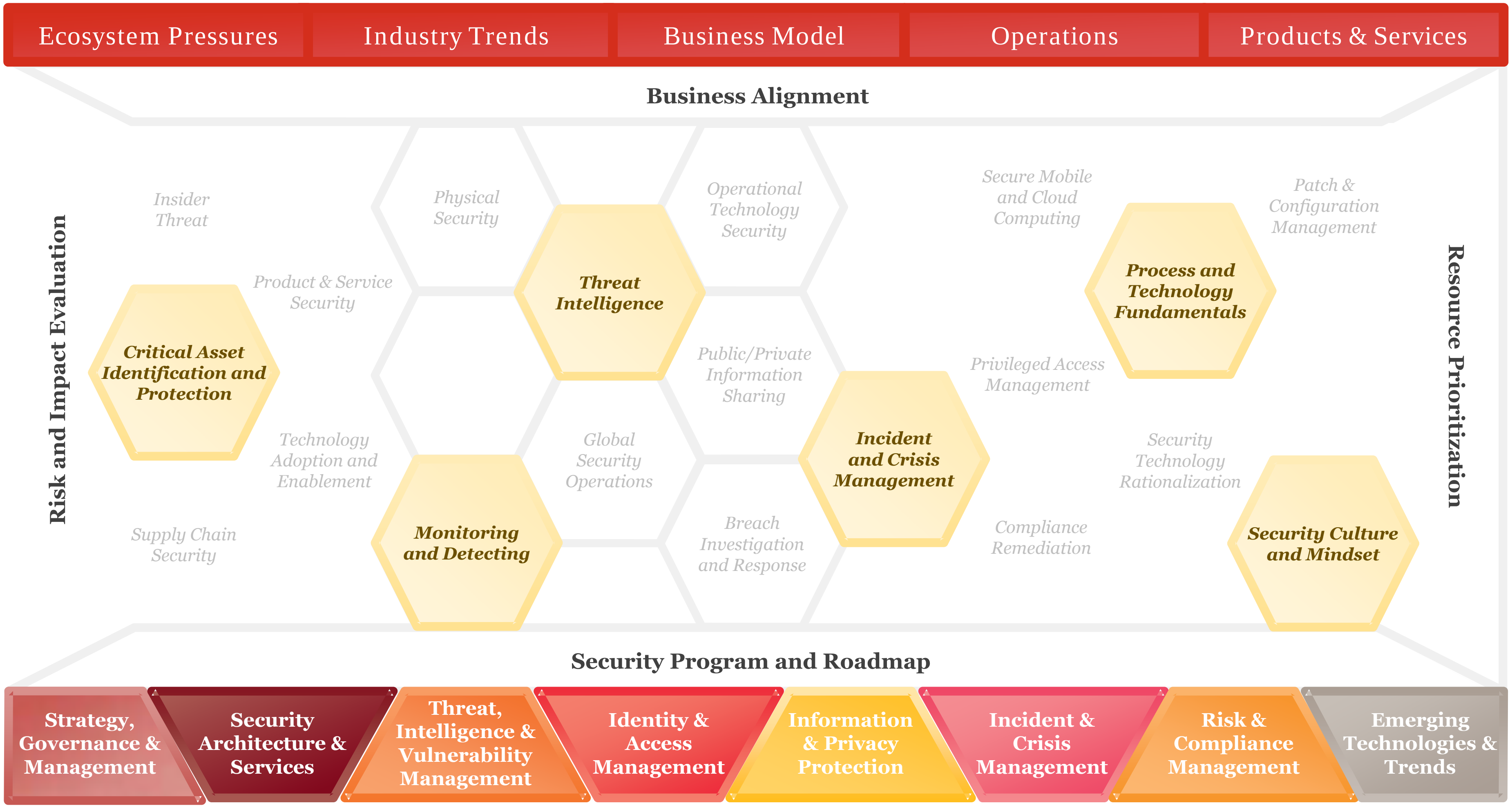
□ MGRS Grid

□ Scale Bar

30.297018°, -114.697266°

Certain areas of underinvestment

Many organization’s ability to adapt and respond to dynamic cyber risks have been impacted by underinvestment in certain areas.



Ecosystem Pressures

Industry Trends

Business Model

Operations

Products & Services

Business Alignment

Risk and Impact Evaluation

Insider Threat

Critical Asset Identification and Protection

Supply Chain Security

Product & Service Security

Technology Adoption and Enablement

Physical Security

Monitoring and Detecting

Threat Intelligence

Global Security Operations

Operational Technology Security

Public/Private Information Sharing

Breach Investigation and Response

Incident and Crisis Management

Secure Mobile and Cloud Computing

Privileged Access Management

Compliance Remediation

Process and Technology Fundamentals

Patch & Configuration Management

Security Technology Rationalization

Security Culture and Mindset

Resource Prioritization

Security Program and Roadmap

Strategy, Governance & Management

Security Architecture & Services

Threat, Intelligence & Vulnerability Management

Identity & Access Management

Information & Privacy Protection

Incident & Crisis Management

Risk & Compliance Management

Emerging Technologies & Trends

Better understanding each of these areas is key to determining your exposure to cyberattacks.

Identify, prioritize, and protect the assets most essential to the business

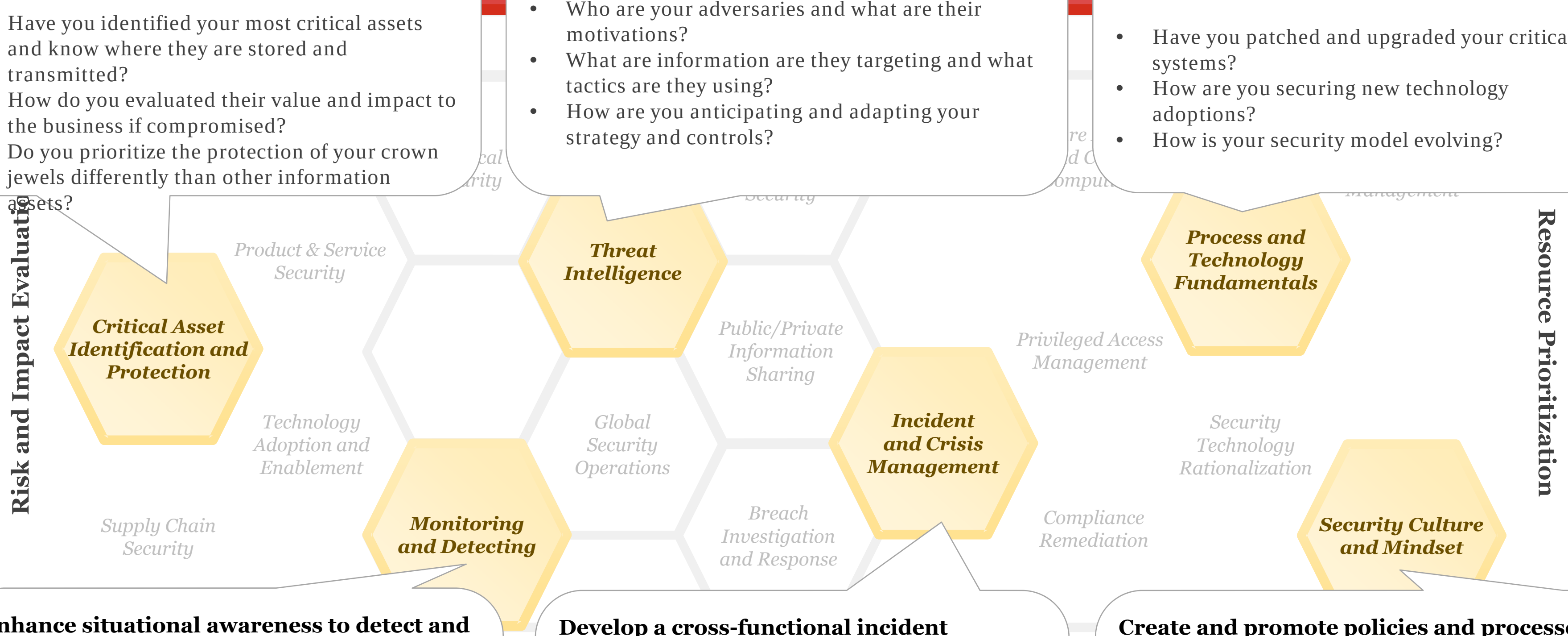
- Have you identified your most critical assets and know where they are stored and transmitted?
- How do you evaluated their value and impact to the business if compromised?
- Do you prioritize the protection of your crown jewels differently than other information assets?

Understand the threats to your industry and your business

- Who are your adversaries and what are their motivations?
- What are information are they targeting and what tactics are they using?
- How are you anticipating and adapting your strategy and controls?

Evaluate and improve effectiveness of existing processes and technologies

- Have you patched and upgraded your critical systems?
- How are you securing new technology adoptions?
- How is your security model evolving?


Risk and Impact Evaluati
Resource Prioritization
Critical Asset Identification and Protection
Product & Service Security
Technology Adoption and Enablement
Supply Chain Security
Threat Intelligence
Public/Private Information Sharing
Global Security Operations
Monitoring and Detecting
Breach Investigation and Response
Incident and Crisis Management
Privileged Access Management
Security Technology Rationalization
Compliance Remediation
Process and Technology Fundamentals
Security Culture and Mindset

Enhance situational awareness to detect and respond to security events

- How are you gaining visibility into internal and external security events and activities?
- Are you applying correlation and analytics to identify patterns or exceptions?
- How do you timely and efficiently determine when to take action?

Develop a cross-functional incident response plan for effective crisis management

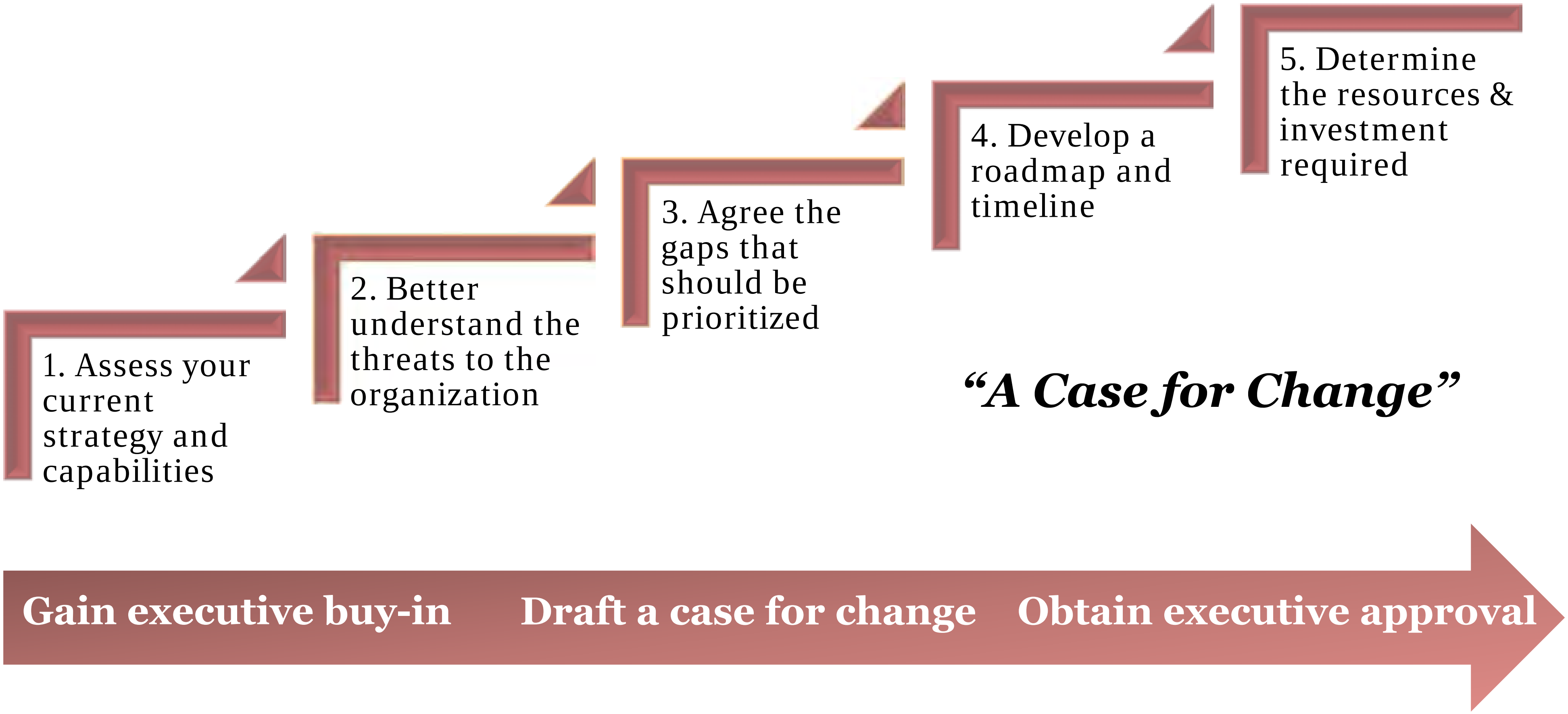
- Have your business leaders undertaken cyberattack scenario planning?
- Do you have a defined cross functional structure, process and capability to respond?
- Are you enhancing and aligning your plan to ongoing business changes?

Create and promote policies and processes to increase security effectiveness

- How are the c-suite and the board engaged in understanding the cyber risks to the business?
- How is your cyber strategy and plan integrated with the business?
- What pervasive cyber training and awareness activities take place?

Reinvesting in Security

Company leaders and boards can no longer afford to underinvest in security nor can they view cybersecurity as a technology problem; the likelihood of a cyberattack is now an enterprise risk management issue.



1. Assess your current strategy and capabilities

2. Better understand the threats to the organization

3. Agree the gaps that should be prioritized

4. Develop a roadmap and timeline

5. Determine the resources & investment required

"A Case for Change"

Gain executive buy-in **Draft a case for change** **Obtain executive approval**

PWC

Q&A: Cyber threats, counter measures and challenges

For more information on cybersecurity…

10Minutes on the stark realities of cybersecurity

pwc

Cybersecurity is more than an IT challenge—it's a business imperative

Changing the game Key findings from The Global State of Information Security® Survey 2013

Key findings from the 2013 US State of Cybercrime Survey

pwc

- www.pwc.com/cybersecurity
  - 10Minutes on the stark realities of cybersecurity (released April 2013) – In your packet
  - Cybersecurity risk on the board's agenda (released April 2013)
  - Cyber Video Series (released February 2013)
- Results of 2014 Global State of Information Security (released September 2013) – In your packet

- What the analysts are saying
  - Forrester: PwC maintains a leadership position through the scope and quality of security service offerings.
  - Gartner: PwC is the #1 global security consulting firm.
  - Kennedy: First annual Cyber ranking due this month.
- Numerous print and television media hits including:
  - WSJ, The NY Times, The Financial Times, CNBC, Bloomberg, Law 360 and a variety of others
- PwC has a national network of state-of-the-art laboratories for IT security testing, research, and data management technologies.

Leading security practices for financial services companies.

Security is a board-level business imperative

Advance your security strategy and capabilities.

- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.
- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.

Board and CEO drive security governance.

- Security risks are operational risks and should be reviewed regularly by the board.
- Strong support and communication from the board and CEO can break down traditional silos, leading to more collaboration and partnerships.

Strong multi-party governance group should manage security risk.

- An executive with direct interaction with the CEO, General Counsel and Chief Risk Officer should lead security governance.
- Security governance group should include representatives from legal, HR, risk, technology, security, communications, and the lines of business.
- The cybersecurity governance group should meet regularly (monthly or quarterly) to discuss the current threat landscape, changes within the organization that impact risk levels, and updates to remediation programs and initiatives.

Security threats are business risks

Security program is threat driven and assumes a continuous state of compromise.

- Security risks are among the top 10 operational risks.
- Adopt the philosophy of an assumed state of compromise, focusing on continuous detection and crisis response in addition to traditional IT security focus of protection and mitigation.
- Security risks include theft of intellectual property, attacks on brand, and social media.
- You should anticipate threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Focus on your adversaries: who might attack the business and their motivations.

Ensure cooperation among third parties.

- Proactively make certain that suppliers, partners, and other third parties know— and agree to adhere to— your security practices.

Leading security practices for financial services companies (cont'd).

Protect the information that really matters	
Identify your most valuable information.	• Know where these “crown jewels” are located and who has access to them. • Allocate and prioritize resources to protect your valuable information.
Establish and test incident-response plans	
Incident response should be aligned at all levels within the organization.	• Incident response should integrate technical and business responses. • Response is aligned at all levels by integrating the technical response (led by IT) and business response (led by business with input from legal, communications, the senior leadership team, and HR).
Security incident response should be tested using real-world scenarios.	• Improve planning and preparedness through table-top simulations of recent industry events and likely attack scenarios. • Frequently conduct table-top simulations. • Response to various attack scenarios and crisis should be pre-scripted in a “play book” format.
Gain advantage through Awareness to Action	
Security is driven by knowledge, an approach we call Awareness to Action.	All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring. • Organizations should create a culture of security that starts with commitment of top executives and cascades to all employees. • Organizations should engage in public-private collaborationwith others for enhanced threat intelligence.

Thank You.

How can PwC help

To have a deeper discussion about cybersecurity, please contact:

Country Contacts:

Gabriel Ukpeh
Partner
+234 (0) 802 778 4967
gabriel.ukpeh@ng.pwc.com

Farouk Gumel
Partner
+234 (0) 803 548 6802
farouk.x.gumel@ng.pwc.com

Daniel Asapokhai
Partner
+234 (0) 802 326 5994
daniel.asapokhai@ng.pwc.com

Femi Tairu
Director
+234 (0) 816 051 4460
olufemi.tairu@ng.pwc.com

Abiodun Adegboye
Associate Director
+234 (0) 8023032773
abiodun.adegboye@ng.pwc.com

Global Contact(s):

David Burg
Principal
Global and US Advisory Cyber Security Leader
+1 703 918 1067
david.b.burg@us.pwc.com

PwC helps organizations and individuals create the value they're looking for. We're a network of firms in 158 countries with more than 180,000 people who are committed to delivering quality in assurance, tax and advisory services. Find out more by visiting us at www.pwc.com.