Deloitte.

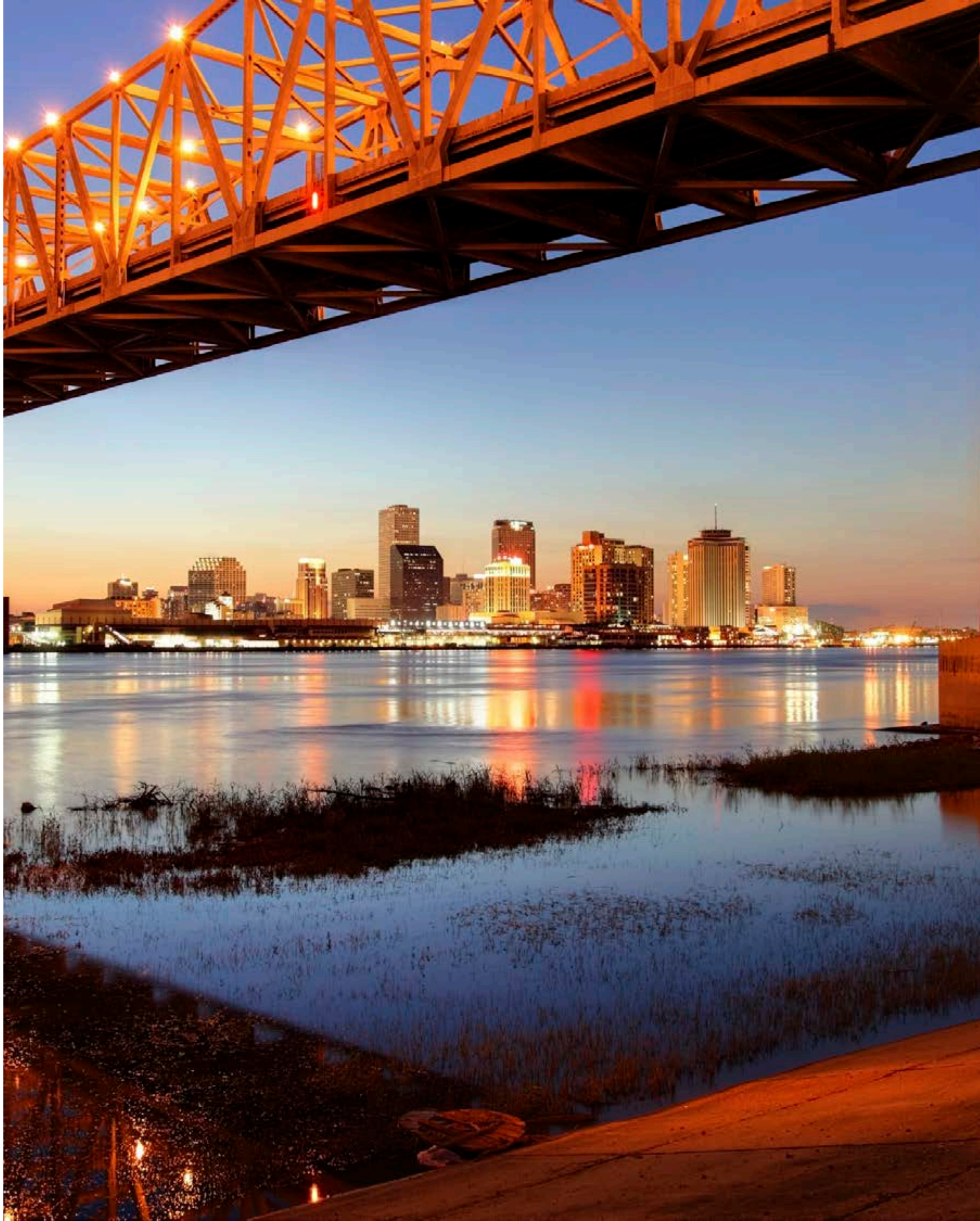
2015 Engineering & Construction Conference

Developing a Business-Centric Cybersecurity Program

C. Kelly Bissell

Deloitte & Touche LLP

June 9, 2015



Background

Who is Kelly Bissell, anyway?

Worked with

25 boards across

Many industries and countries.

Sees many good/bad ways of reporting

Advising the NSA

Has spent

28 years

fighting cyber crime – half of this in industry

Runs

Deloitte's global cyber practice. He sees cyber risks across the globe

Deloitte Risk Consulting & Implementation Services

More than

93,000

professionals

100 offices

in more than

34 countries

Offering:

- Strategy & Operations
- Implementation
- Managed Services

US $19.4B

in revenue

Deloitte Cyber Risk Services

Deloitte leverages an array of geographically distributed delivery centers with tools, frameworks, and methodologies to enable integrated delivery

More than

1,787

US Cyber Risk professionals and over

3,400

resources worldwide

Engaged on over

2,400

Global Cyber Risk projects

- "Gartner ranks Deloitte #1 for Information Security Consulting Services Worldwide, based on market share, in 2013."

  Source: Gartner, Market Share Analysis: Information Security Consulting, Worldwide, 2013, Jacqueline Heng, Lawrence Pingree, 16 May 2014

- Named as a Kennedy Vanguard Leader in cyber security consulting: "[Deloitte] continually develops, tests, and launches methodologies that reflect a deep understanding of clients' cyber security and help the firm… set the bar."

  Source: Kennedy Consulting Research & Advisory; Cyber Security Consulting 2013; Kennedy Consulting Research & Advisory estimates © 2013 Kennedy Information, LLC. Reproduced under license.

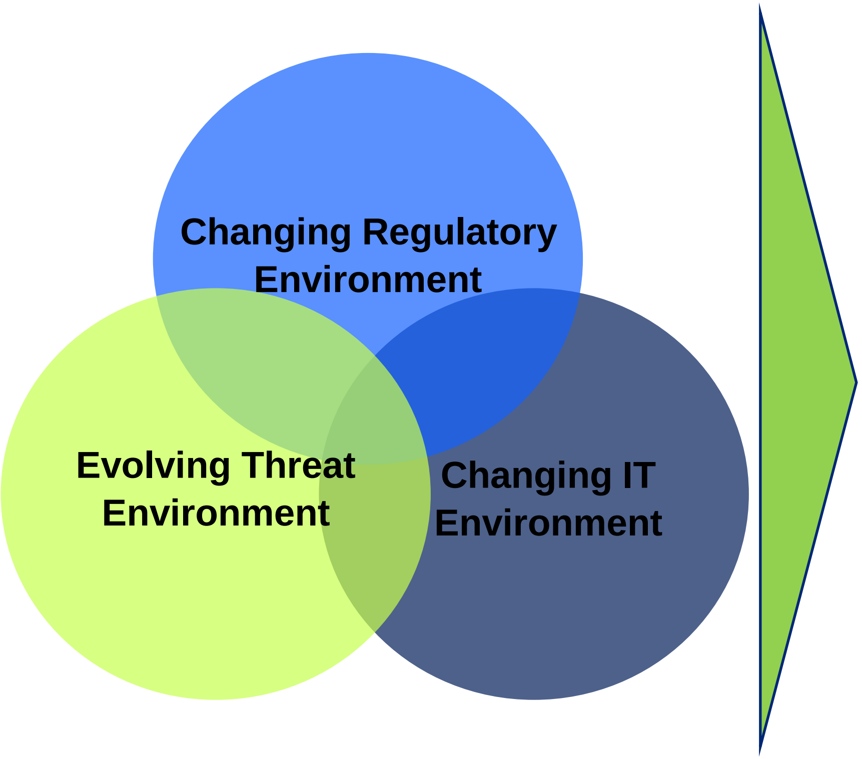
- "Deloitte's *ability to execute rated the highest* of all the participants"

  Forrester Research, "Forrester Wave^{TM}: Information Security Consulting Services Q1 2013", Ed Ferrara and Andrew Rose, February 1, 2013

Discussion topic for today

1. Level set on the Cyber risk landscape
2. Building an **effective** Cyber Risk program:
   - What to plan for
   - What do bad guys want from you
   - A framework for building
   - 5 common questions you should ask yourselves when defining the program
3. Other topics?

What is new with Cybersecurity?



The business and IT environment is changing…

- New business models – cloud, mobile
- Enterprise IT environment disrupted – BYOD & "rogue IT"
- Regulatory changes with SEC rules, state & country laws, industry regulation, emerging NIST standards, EU, and more.

…Leading to new, persistent, evolving risks…

- More frequent, sophisticated & malicious attacks
- Wide range of motives: economic, campaigns, Hactivists
- Hackers already inside the organization
- Data easily available and it's money
- C-Suite, Board, and key staff are sitting targets

…Clients are struggling to keep pace:

- Risks are evolving faster than clients can react
- Need to transform how they think about Cybersecurity
- Companies large and small do not have the skills in-house
- Greater need for comprehensive, enterprise solutions
- Boards and Management are struggling how to "measure" cyber risk

We still live in a dangerous world…

$53B

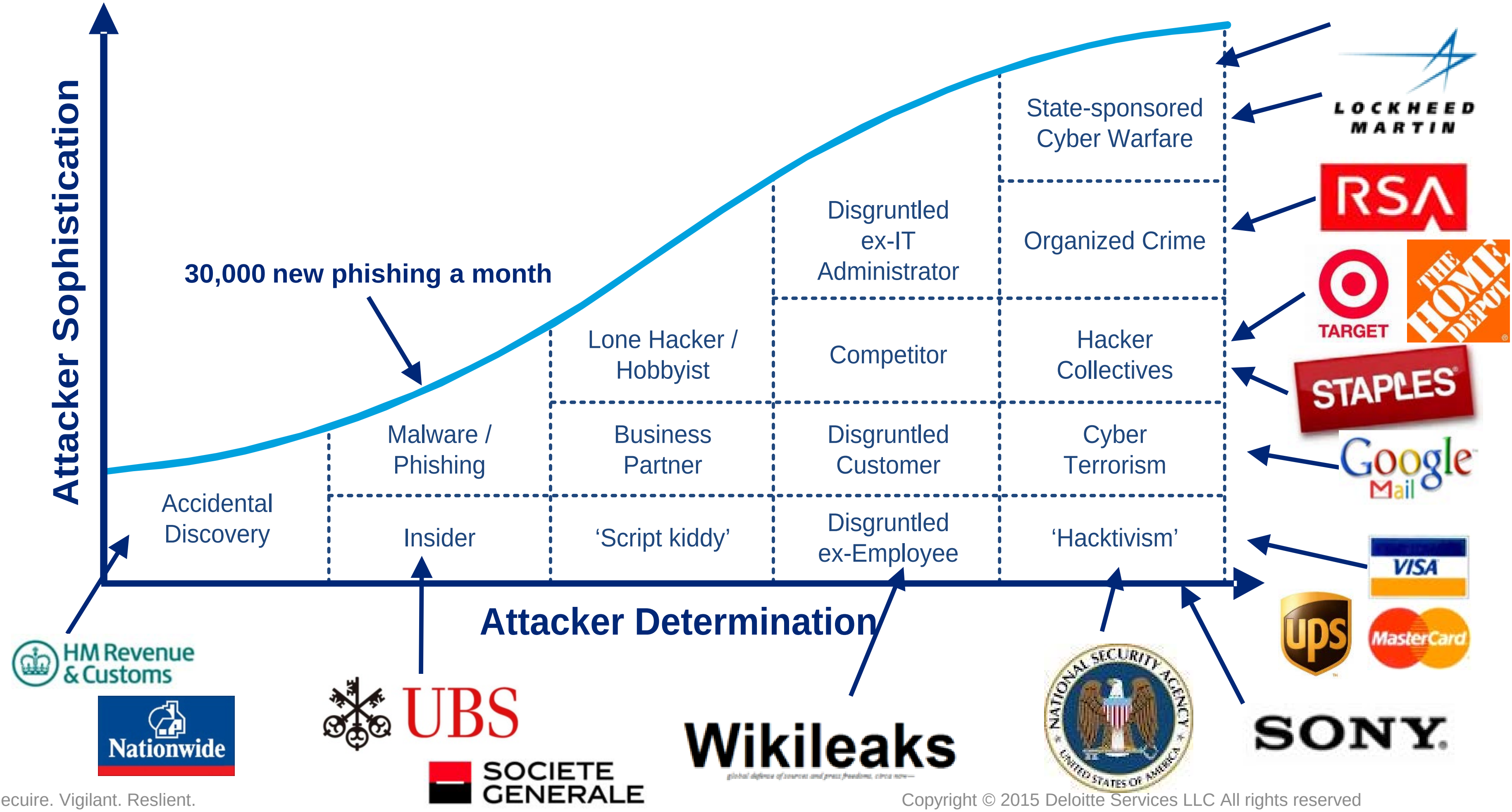
Market

- **Companies are always under attack. The wolves do not rest**
- **We have no more borders**
- **To be safe, we have to be Secure, Vigilant and Resilient.**

Don’t forget the wolf in sheep’s clothing

How are attacks occurring across the market?

It is important for all employees, contractors and suppliers to be aware of how bad guys target us for carrying out well-planned attacks and what it could mean to our businesses.


Attacker Sophistication

Attacker Determination

30,000 new phishing a month

Accidental Discovery

Malware / Phishing

Insider

Lone Hacker / Hobbyist

Business Partner

'Script kiddy'

Disgruntled ex-IT Administrator

Competitor

Disgruntled Customer

Disgruntled ex-Employee

State-sponsored Cyber Warfare

Organized Crime

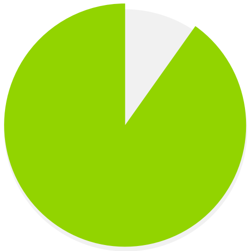
Hacker Collectives

Cyber Terrorism

'Hacktivism'

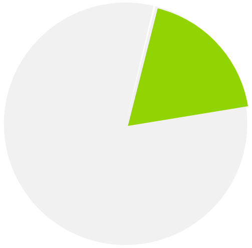
Breaches are a multi-faceted problem

Any one-dimensional attempt to describe them fails to adequately capture their complexity



92%

Of breaches are perpetrated by outsiders



14%*

Of breaches are by insiders and are *rising*

76%

of incidents are caused by weak or stolen credentials. Rogue hardware and malware are also frequent causes.

Known External Actors

55%

Organized Crime

21%

State affiliated

2%

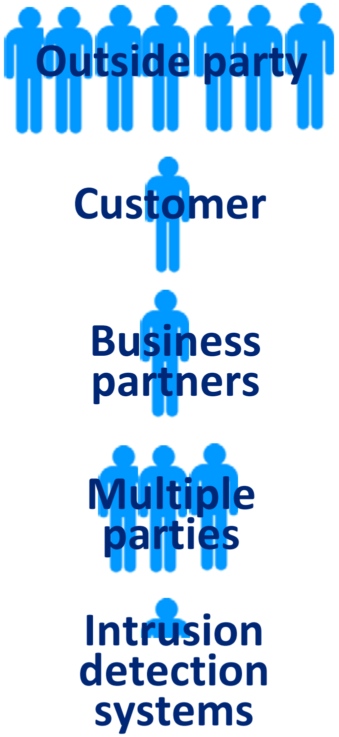
Activist

1%

Former employee

95% **of state actors use Phishing**

Who found the incident



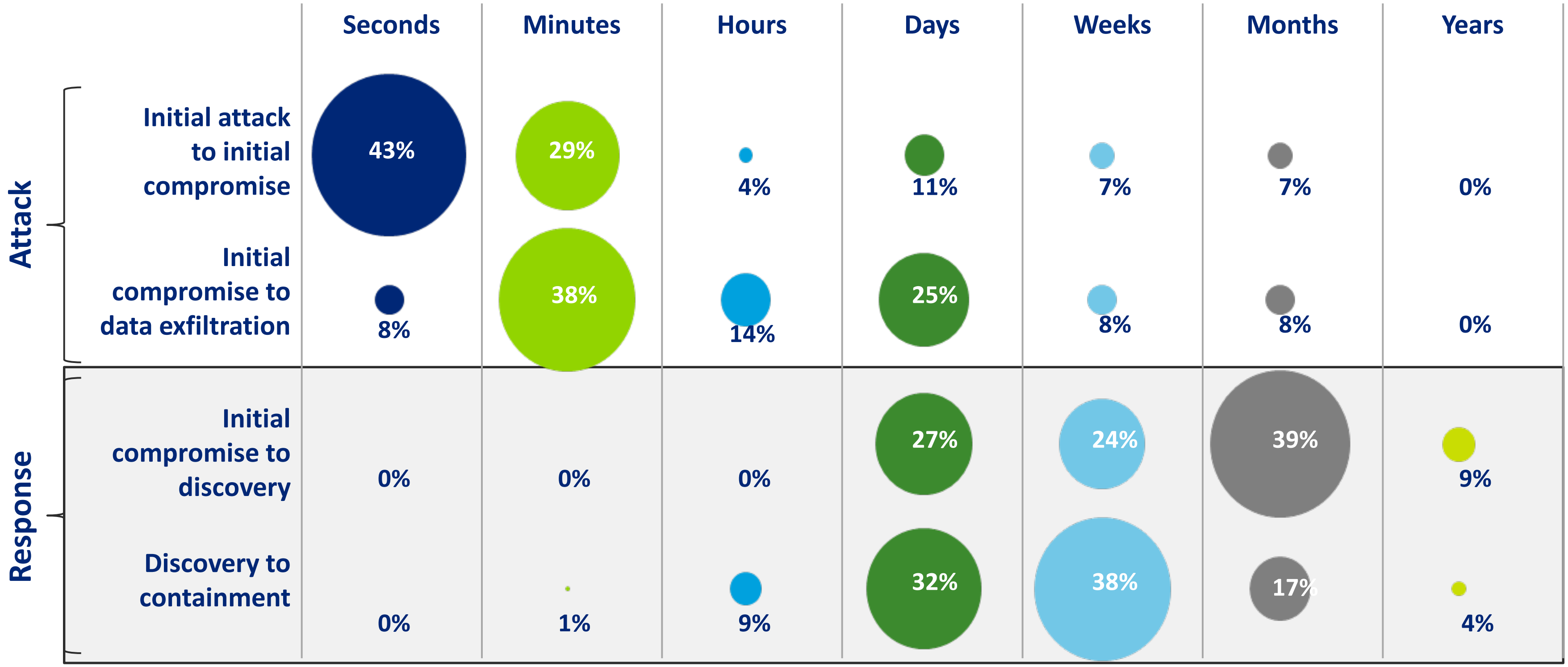
Source: 2014 Verizon Data Breach Investigations Report with the U.S. Secret Service, FBI, Deloitte, DHS and others
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2014_en_xg.pdf

* number overlap because some insiders and outsiders are in collusion

The need for speed

- The frequency of cyber attacks is steadily increasing. Attackers have a **limitless number of attempts** to compromise your defences, but **it only takes a single weakness** on your part to get in.

- Businesses have to accept that it **is not possible to prevent all cyber attacks**. However, you can still significantly limit damage by quickly identifying and dealing with any compromise.



		Seconds	Minutes	Hours	Days	Weeks	Months	Years
Attack	Initial attack to initial compromise	43%	29%	4%	11%	7%	7%	0%
	Initial compromise to data exfiltration	8%	38%	14%	25%	8%	8%	0%
Response	Initial compromise to discovery	0%	0%	0%	27%	24%	39%	9%
	Discovery to containment	0%	1%	9%	32%	38%	17%	4%

Developing a business-based Cyber program.

Plans should focus on answering key questions that should be addressed by an effective Cyber Risk strategy

Gov & Oversight

Governance & oversight

- Who is responsible and accountable for cyber risk across and within our businesses and enabling areas?
- Who are the key stakeholders and how do they work together to enhance our cyber risk program?
- How do we choose the right programs and processes? What is the role of technology?
- How do we effectively communicate key cyber risk metrics to leadership to drive informed decisions?

Secure.Vigilant.Resilient™

Secure

Secure

- How do we secure our most critical information and other assets against our most significant threats?
- What controls are imperative to implement/enhance in the near term, mid term, and long term?
- How do we create a more "security aware" culture across the company?

Vigilant

Vigilant

- How do we enhance our ability to monitor for known threats?
- How do we design systems and processes to detect emerging threats?
- How we develop capabilities to predict future threats?

Resilient

Resilient

- How can we adapt our crisis management capabilities to different types of cyber incidents?
- How do we triage attacks and rapidly restore operations with minimal service disruption?
- How do we enhance systems and processes to withstand disruption for extended periods?
- What is the role of cyber insurance to mitigate losses from cyber incidents and data breaches?
- How can cyber simulations help us evaluate and improve our cyber preparedness?

Every company has a different risk tolerance and different threat model. This has to be tailored to each company.

Sample Threat Profile for E&C companies

Functions ACTORS	Financial Systems or back office	Design & Build	Demolition	Construction Management (GC and Sub)	Environmental, HVAC, Watershed, and Energy Systems	Property Management
Organized criminals	• IP Theft • SSN theft	• IP Theft • SSN theft	•Individual Targeting	•Supply Chain interrupt		•Tenant targeting
Hactivists		• Systems de-facing	•Systems de-facing	•Supply Chain Interrupt	• Systems de-facing	•Systems de-facing • Energy interruption
Nation states		• Design plans • Raw materials bid / forecasting		• Design plans • Raw materials bid / forecasting		
Insiders / Partners	•Account fraud •Upstream attack	•System damage • Upstream attack		•Systems damage •Upstream attack		
Competitors	•Bid Contract / Proposal data •Pricing plans	•Bid Contract / Proposal data •Pricing/Estimating models	•Bid Contract / Proposal data •Pricing/Estimating models	•Construction disruption		
Cyber Terrorists				•Construction disruption •Supply chain interruption	•SCADA interruption	
Skilled individual hackers	•ACH/Wire fraud •Front Running •M&A info	•Access to SCADA or access control systems			•Access to SCADA or access control systems	•Tenant targeting

KEY

■ Very high

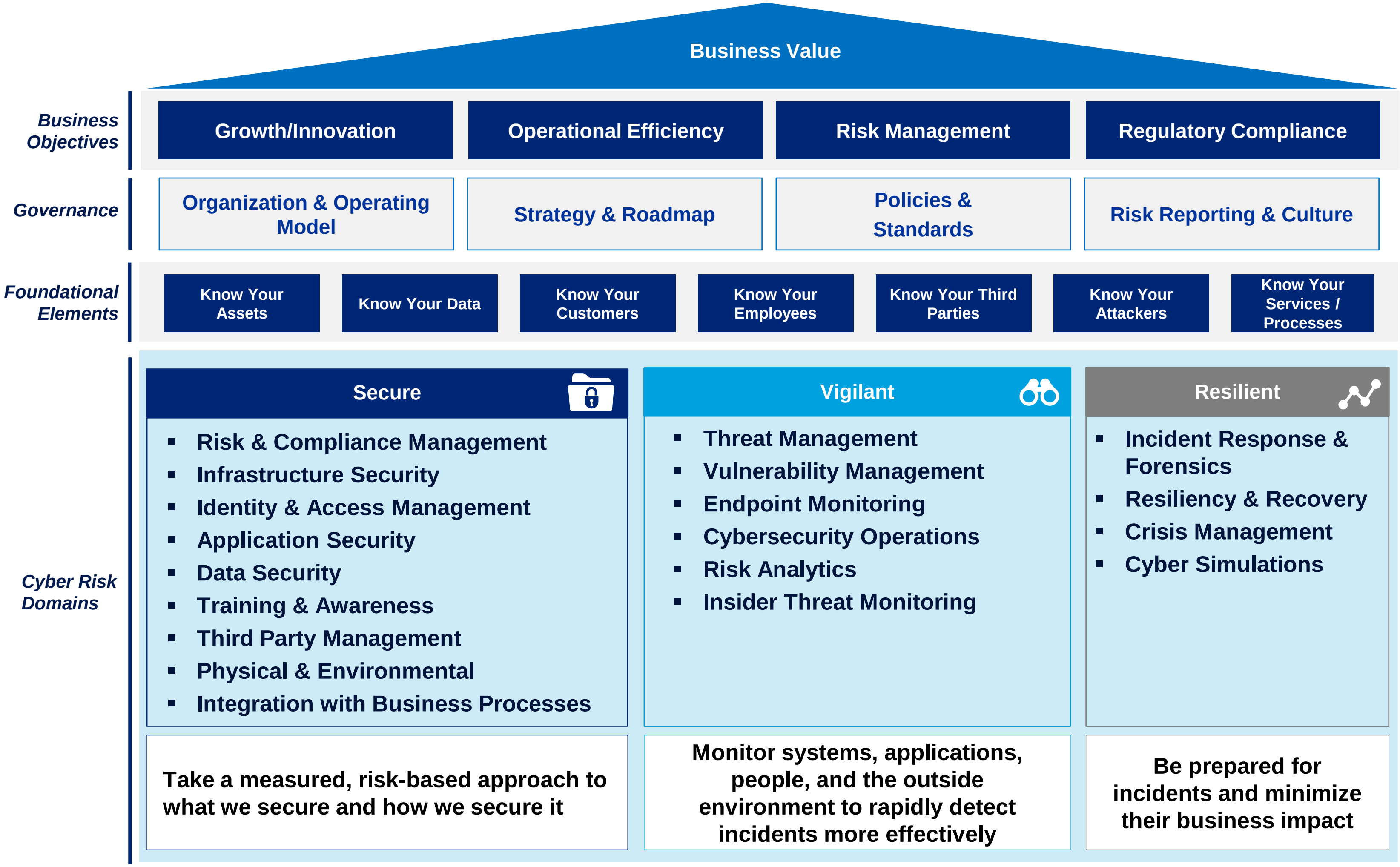
■ High

□ Moderate

□ Low

Cyber Risk Management Framework

Company needs to more fully implement a comprehensive framework to effectively manage cyber risks. We have used Deloitte's Secure.Vigilant.Resilient framework for the current state assessment. This framework is built upon industry standards, leading practices and lessons learned from cyber crises.



Business Value

Business Objectives

- Growth/Innovation
- Operational Efficiency
- Risk Management
- Regulatory Compliance

Governance

- Organization & Operating Model
- Strategy & Roadmap
- Policies & Standards
- Risk Reporting & Culture

Foundational Elements

- Know Your Assets
- Know Your Data
- Know Your Customers
- Know Your Employees
- Know Your Third Parties
- Know Your Attackers
- Know Your Services / Processes

Cyber Risk Domains

Secure

- Risk & Compliance Management
- Infrastructure Security
- Identity & Access Management
- Application Security
- Data Security
- Training & Awareness
- Third Party Management
- Physical & Environmental
- Integration with Business Processes

Take a measured, risk-based approach to what we secure and how we secure it

Vigilant

- Threat Management
- Vulnerability Management
- Endpoint Monitoring
- Cybersecurity Operations
- Risk Analytics
- Insider Threat Monitoring

Monitor systems, applications, people, and the outside environment to rapidly detect incidents more effectively

Resilient

- Incident Response & Forensics
- Resiliency & Recovery
- Crisis Management
- Cyber Simulations

Be prepared for incidents and minimize their business impact

Five common questions from the board, four key controls for executives

Key questions the Boards are talk with management

1. **Are we focused on the right things?**
   Often said, but hard to execute. Understand how value is created in your organization, where your critical assets (aka Crown Jewels) are, how they are vulnerable to key threats. Practice defense-in-depth. Are we learning from other breaches?

2. **How are you measuring cyber risks?**
   Please stop give us project status. Instead tell us how are you measuring cyber risks as the business changes? What are the "metrics that matter" and what is our cyber risk tolerance?

3. **Do we have the right talent?**
   Quality over quantity. There is not enough talent to do everything in-house, so take a strategic approach to sourcing decisions (e.g. teaming with others).

4. **Are we incentivizing openness and collaboration?**
   Strong relationships with partners, law enforcement, regulators, and vendors. Foster internal cooperation across groups and functions, and ensure that people aren't hiding risks to protect themselves.

5. **Are we ready for a breach?**
   Have we done more than a table-top exercise but a real test (simulation) with client management, logistics, marketing, PR, IT, etc.? Has this been validated with a 3rd party?

Common Key IT controls deficiencies that give way to breaches

1. **Privileged & User Management:**
   Privileged users are ones who have the most powerful access to systems and databases where our data is stored. These users need this access to maintain the systems. In hands of bad guys, all the data can be copied, changed, or destroyed. Important to auto-terminate user access once they leave.

2. **Patch Management:**
   All systems have vulnerabilities or holes that allow for bad guys to get in. Almost daily, "patches" are created to close these holes in the systems. As an IT group we need to evaluate these patches for applicability and apply them as quickly as possible without breaking the functionality of our systems.

3. **Application Testing:**
   Much with system patches, IT groups unknowingly create ways for bad guys to get in through our applications that help manage our business.

4. **External & Internal Monitoring:**
   With increasing sophistication and examples of highly "secure" companies breached such as NSA, Google, Apple, Target, Home Depot, Ford, and many others, companies should build better defenses but also focus more on Detection inside the network and systems and 3rd parties.

Appendix

Other industry cyber threat profiles

Sample Threat Profile for Airlines

Functions ACTORS	Financial Systems or back office	Reservations & GDS ecosystem	PNR data	Flight Operations	Fuel Logistics	Airport Ops (retail, security checks, bag drop, etc)	Ramp & Tarmac Operations	Airfield Operations & Maint.
Organized criminals	• IP Theft • SSN theft	• IP Theft • SSN theft	• Individual Targeting	• Supply Chain interrupt				
Hactivists				• Supply Chain Interrupt	• Supply Chain Interrupt	• Systems de-facing		
Nation states								
Insiders / Partners	• Account fraud • Upstream attack	• System damage • Upstream attack		• Systems damage • Upstream attack				
Competitors	• Contract / Proposal data • Pricing plans	• Contract / Proposal data						
Cyber Terrorists				• Flight disruption	• Fuel disruption	• SCADA interruption • Passenger targeting	• Logistics interruption	• Airfield damage for flight interruptions
Skilled individual hackers	• ACH/Wire fraud • Front Running • M&A info	• ACH/Wire fraud • Front Running • M&A info	• FF Account takeover		• Fuel hedge positions			

KEY

■	Very high	▧	Moderate
▩	High	□	Low

Threat actors and their motives vary by industry and organization

A typical cyber risk heat map for the Automotive sector

Notable insights:

- While risks posed to sensitive intellectual property and other sensitive company data are important, senior leaders become equally concerned about end-point risks at the smart vehicle and loss of client / investor confidence.
- Concern has shifted to nation-states, global organized criminal gangs and highly skilled hactivists or hackers.
- Targeted, blended, low-and-slow-style attacks are designed to appear as “normal” activity, eluding detection by signature-based technologies.
- Cyber dependencies across the ecosystem between automobile companies, critical suppliers, industry partners, vehicles, etc., introduce high levels of third party risks, insider risks, and social media risks.

IMPACTS ACTORS	Financial theft / fraud	Theft of IP or strategic plans	Business disruption	Data Gathering/ Marketing	Reputation damage	Threats to life / safety	Vehicle theft / fraud
Organized criminals	█	▓	█	░	▒	█	█
Hactivists	▒	▒	█	▓	█	▓	▒
Nation states	▒	█	▓	█	▒	█	▒
Insiders / Partners	▒	█	▓	█	█	░	▓
Competitors	░	█	▒	█	▒	░	░
Skilled individual hackers	░	▒	░	█	▒	▒	▒

KEY

█ **Very high** ▒ **Moderate**
▓ **High** ░ **Low**

Threat actors and their motives vary by industry and organization

A typical cyber risk heat map for the Banking sector

Notable insights:

- Concern has shifted to nation-states, global organized criminal gangs and highly skilled hactivists or hackers.
- While financial risks are important, senior leaders are more worried about destructive attacks and loss of client / investor confidence.
- Concern about harm not only to individual organizations but also about system risks to the US economy via a concerted cyber attack. Cyber attacks may be a particular risk during times of conventional war or international crisis.
- Cyber dependencies across the ecosystem between financial institutions, critical suppliers, industry partners, etc. introduce high levels of third party risks, insider risks, social media risks, etc.

IMPACTS ACTORS	Financial theft / fraud	Theft of IP or strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life / safety	Regulatory
Organized criminals	⬛	▒	□	□	⬛	▩	⬛
Hactivists	▩	▒	⬛	▩	⬛	□	▩
Nation states	▩	⬛	⬛	⬛	⬛	□	⬛
Insiders / Partners	⬛	▩	▩	▒	▩	▒	▩
Competitors	□	▒	□	□	□	□	□
Skilled individual hackers	⬛	▩	▩	▩	▩	□	▩

KEY

⬛	Very high	▒	Moderate
▩	High	□	Low

Threat actors and their motives vary by industry and organization

A typical cyber risk heat map for the Retail sector

Notable insights:

- Recent cyber attacks highlight the urgency for retail organizations to contend with ever increasing risks to customer protection, continuity, fiduciary responsibility and operations.
- Cyber issues can lead to brand degradation and change in consumer behavior.
- Attacks are exploiting weaknesses in traditional controls, some very destructive. Traditional controls around Point of Sale and other IT systems are necessary, but may no longer be adequate.
- Many retailers tend to take a compliance-driven approach (e.g., Payment Card Industry or PCI).

IMPACTS ACTORS	Financial theft / fraud	Theft of IP or strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life / safety	Regulatory
Organized criminals	■	□	▩	□	■	□	■
Hactivists	□	□	▨	□	▨	□	▨
Nation states	□	□	▨	□	▨	□	▩
Insiders / Partners	▩	▩	▩	□	▩	□	▩
Competitors	□	▩	□	□	▨	□	□
Skilled individual hackers	■	▨	▩	□	■	□	■

KEY

■	Very high	▨	Moderate
▩	High	□	Low

Threat actors and their motives vary by industry and organization

A typical cyber risk heat map for the Travel, Hospitality and Leisure sector

Notable insights:

- Concern has shifted to nation-states, global organized crime, and the potential for these actors to collaborate with insiders and business partners.
- While financial risks are important, senior leaders are increasingly concerned about reputation damage and loss of client / investor confidence and trust.
- Concern about harm not only to individual organizations but also about loss of customer personally identifiable information (PII) and customer travel and leisure preference data via a concerted cyber attack.

IMPACTS ACTORS	Financial theft / fraud	Theft of IP or strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life / safety	Loss of customer data
Organized criminals	■	▦	▒	□	□	□	■
Hactivists	■	▦	▦	□	▦	□	■
Nation states	□	▒	■	□	■	□	▦
Insiders / Partners	■	□	▦	□	▦	□	■
Competitors	□	□	□	□	□	□	□
Skilled individual hackers	□	□	▦	□	□	□	□

KEY

■ Very high ▒ Moderate

▦ High □ Low

Threat actors and their motives vary by industry and organization

A typical cyber risk heat map for the Life Sciences sector

Notable insights:

- Concern primarily arises from threat actors on the inside, hacktivists and nation-states.
- Data sharing and intellectual property (IP) risk from third parties are acute due to complex ecosystem of marketing authorization holders and third party intermediaries such as contract researchers, manufacturers and distributors.
- Impacts are amplified by heavy reliance on outsourced IT operations and intricate in-license and out-license agreements with competitors.
- Decentralized governance over and geographic dispersion of physical supply chain and technological operations can weaken cyber command and control.
- General lack of overall industry maturity in cyber domains results in life sciences companies which may be ill-prepared targets.

IMPACTS ACTORS	Financial theft / fraud	Theft of IP or strategic plans	Business disruption	Mfg. & Dist. Infrastructure Disruption	Reputation damage	Threats to life safety	Regulatory issues
Organized criminals	▒	▒	░	▒	▒	▓	░
Hactivists	░	▒	■	▓	■	▒	▒
Nation states	░	■	░	▒	▓	░	░
Insiders / Delivery sites	■	■	▒	▓	■	▒	▒
Competitors	░	▓	░	░	▓	░	░
Skilled individual hackers	░	▒	░	░	▒	▓	░

KEY

■	Very high	▒	Moderate
▓	High	░	Low

Threat actors and their motives vary by industry and organization

A typical cyber risk heat map for State Government

Notable insights:

- Cybercriminals and hacktivists use increasingly sophisticated methods and rapidly evolving technologies to target cyber infrastructure for monetary gain and make political statements.[1]
- Insufficient funding is still the greatest hurdle CISOs face.[1]
- When personally identifiable information (PII) goes public, it can spur some of the most heated citizen outrage and damning media attention.[1]
- The costs of breaches are substantial. The annual Ponemon study[2] puts the organizational cost per breach at $5.5 million – a hefty penalty that financially strapped states can little afford.
- Emerging cybercrime and state-sponsored threats will require a strong response from states.

IMPACTS ACTORS	Financial theft / fraud	Theft of IP or strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life safety	Regulatory
Organized criminals	■	□	□	□	▩	□	□
Hactivists	□	□	■	□	■	□	□
Nation states	□	□	■	▦	□	□	□
Insiders / Partners	■	□	▩	□	▩	□	□
Competitors							□
Skilled individual hackers	▦	□	▩	□	▩	□	□

KEY

■	Very high	▦	Moderate
▩	High	□	Low

Sources:

[1] http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2012.pdf

[2] "2011 Cost of Data Breach Study: Global." Ponemon Institute. March 2012.

Conference Resources

A copy of this presentation may be downloaded from the conference website.

To access this presentation – and all other presentations from this conference, please use the following url:

www2.deloitte.com/us/2015ECConference

You may also access all presentations and thoughtware through our conference app

Deloitte.

This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.