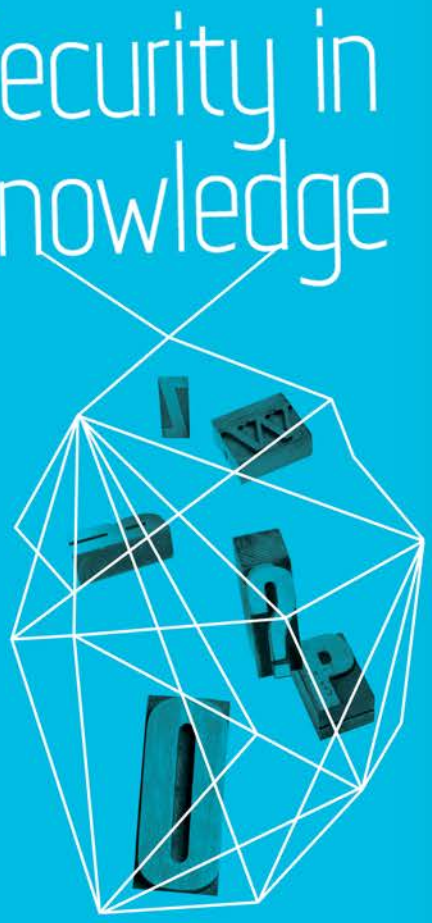
RSA CONFERENCE ASIA PACIFIC 2013

ASSUMING A STATE OF COMPROMISE: EFFECTIVE DETECTION OF SECURITY BREACHES



Leonard Levy
PricewaterhouseCoopers LLP

Session ID: SEC-W03

Session Classification: Intermediate

pwc

Agenda

- The opportunity
- Assuming a state of compromise
- Incremental capabilities needed
- Case studies of actual incidents

The opportunity

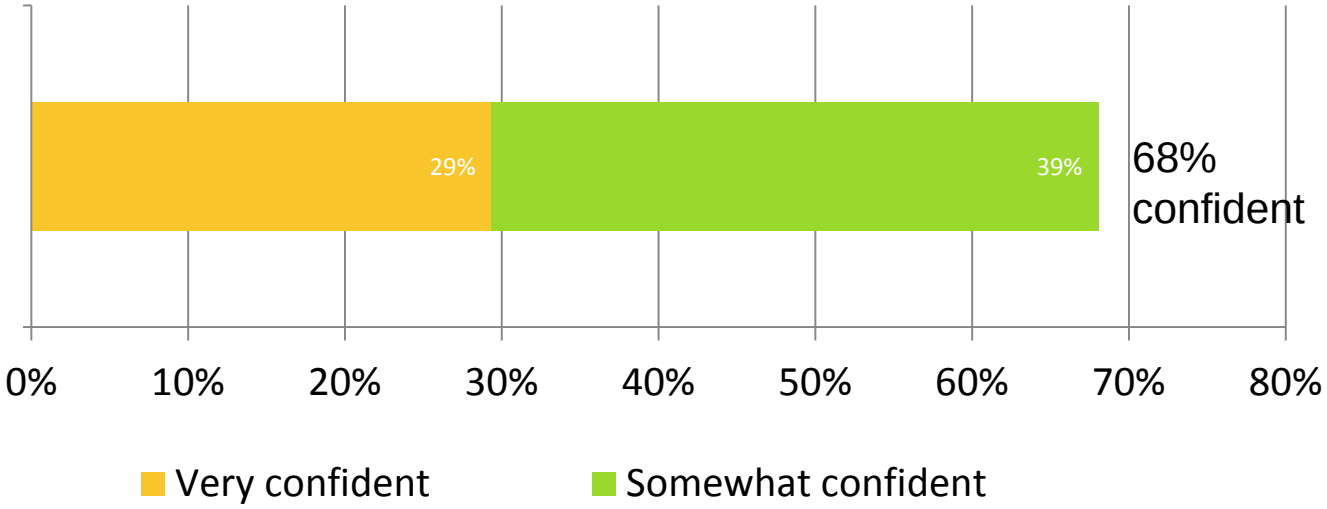
Confidence is high

42% of respondents say their organization have a strategy in place and is proactive in executing it—exhibiting two distinctive attributes of a leader.

Source: The Global State of Information Security® Survey Question 28 - "Which category below best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding.)

Information security behaviors

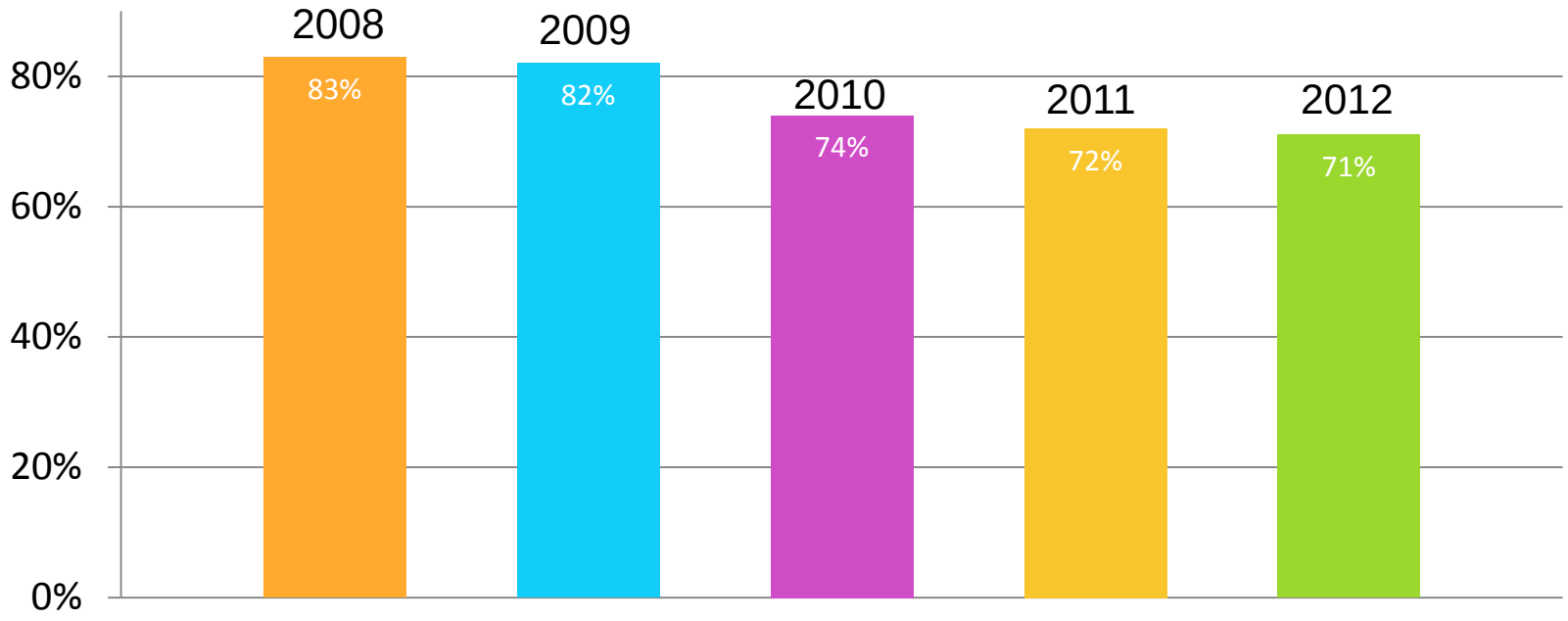
To be effective, security must be integral to the way people think and work, not just another item to be checked off a list. 68% of respondents are either very or somewhat confident they have instilled effective security behaviors into their organizational culture.



Source: The Global State of Information Security® Survey Question 35 - "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?" (Not all factors shown. Totals do not add up to 100%.)

Yet confidence is eroding…

Confidence is a good thing. More than 70% of respondents are very (32%) or somewhat (39%) confident that their organization's information security activities are effective. Yet they may not realize that assurance has dropped since 2008.



Source: The Global State of Information Security® Survey Question 41 - "How confident are you that your organization's information security activities are effective?"

Why is confidence eroding?

- New adversaries.
- The cost of attacks is low.
- Successful attack requires just one vulnerable spot for success.
- The defenders are required to **protecting everything** equally, which is not cost-effective.
- Investment in security controls is based on known vulnerabilities or “vendor buzz”.

Key barriers to effective security

- Cyber security is still pigeon-holed as an IT issue, creating a communications gap between managers in the business and the security teams.
- The people engaged in securing cyber space face the challenge of continuing to raise their game faster than the attackers.
- Traditional organisational structures tend to be too slow and rigid to enable the speed and flexibility of response needed in the cyber world.

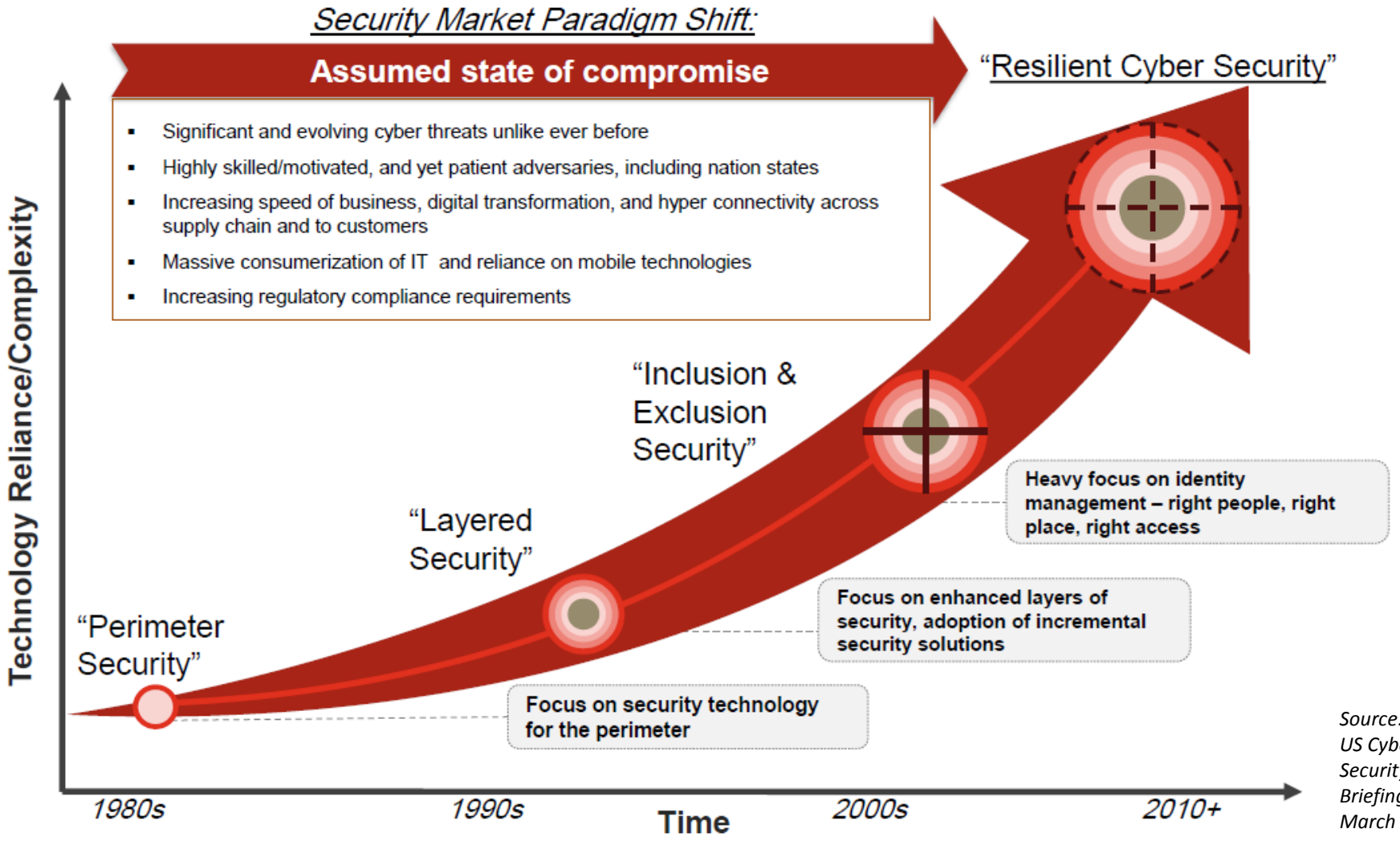
- ✓ *Cyber opportunities are overseen by a variety of C-level executives with the CIO being the single most common owner.*
- ✓ *Cyber risks are owned either by the Chief Risk Officer or Chief Information Security Officer.*
- ✓ *The CEO is still relatively uninvolved in either area.*

Ref: PwC / ISF June 2011

The need for change

The future of cyber security is going to require an evolved philosophy that assumes a never-ending state of compromise.

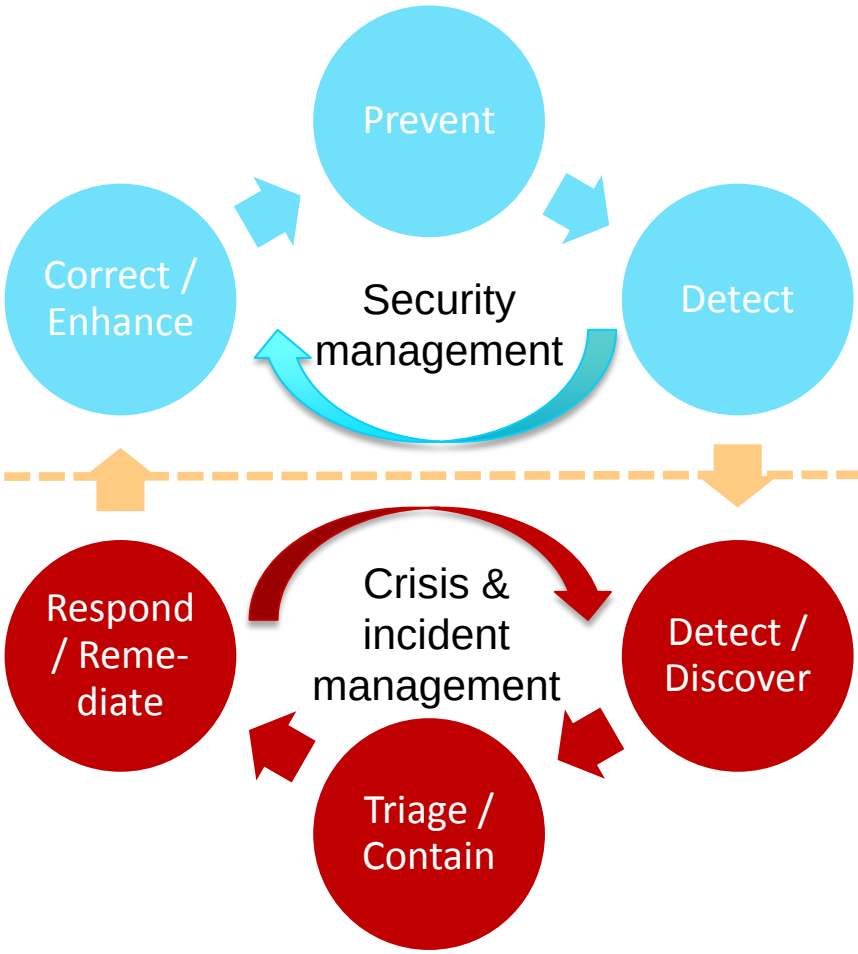
Resilient Cyber Security



Source: PwC US Cyber Security Briefing March 2013

Cyber evolution

Traditional security lifecycle



State of compromise

Holistic approach for dealing with increased volume, complexity, and detection difficulty of attacks.

Source: PwC UK Cyber Threat Landscape April 2013

Focusing resources and effort

What it is not	What it is
Additional investment in new technology	A modern viewpoint on budget allocation priorities, with smarter investment decisions driving more effective detection, response and containment of inevitable advanced threats
A silver bullet to prevent breaches	An approach to help organisations detect breaches earlier in their lifecycle, before they impact the business, and a methodology to ensure they are dealt with swiftly and calmly
A technology-specific solution	Enterprise crisis readiness and crisis management combined with threat intelligence to understand relevant risks and mitigate associated business impacts
A point-in-time or “set and forget” fix	A business-as-usual methodology and approach

Invest where it matters

The question has always **been where we should invest our resources** – but with a constantly changing landscape of Attackers and Vulnerabilities, reacting is no longer enough.

- While keeping up to date is important, checking to see **if new threats are relevant to you**, and where you should invest within your setup is critical.
- We need to be able to adjust to new understanding of risk on **a much shorter time-scale**.

All this via the perspective of what the **business impact** of a threat may be.

Assuming a state of compromise

New mind-set: assume compromise

Basic **breach indicators** of an active cyber intrusion can include:

- Data transmitting outbound over unlikely protocols
- Large compressed files being transmitted outbound
- Unusual connections between a user systems using native operating system networking features
- Log entries on domain controllers capturing the execution of unauthorized programs
- Unauthorized processes running on key executives' PC
- Unauthorized web pages created on an Internet-facing web server

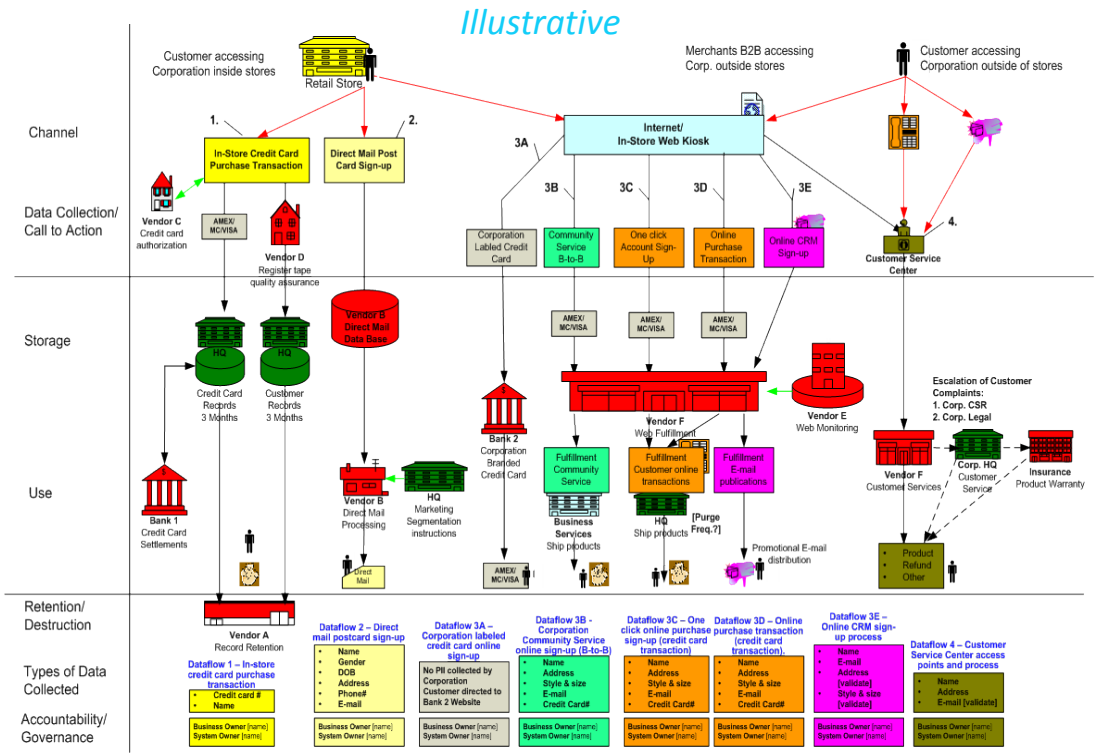
Recognition of advanced cyber intrusions is often through third-party tipsters such as domestic law enforcement, intelligence sources, customers, or business partners.

Identify breach indicators

Phase 1

Understand where the “valuable” data is stored

- Structured and Unstructured
- What would an attack target
- Update your IT asset inventory



Identify breach indicators

Phase 2

Investigate the environment for network and system breach indicators:

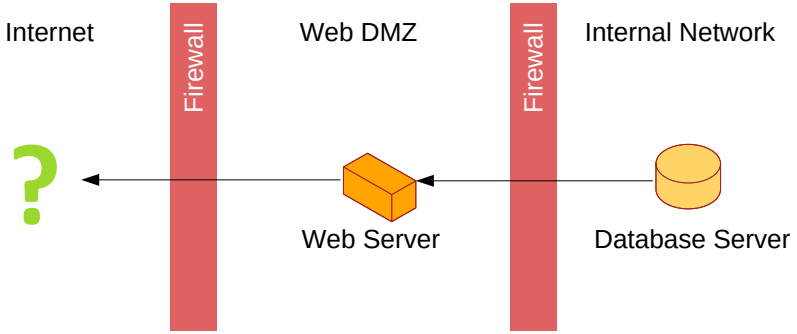
- Develop system and network baselines
  - Based on your own environment
  - Based on standards for your technology and industry
- Review both system and network activity
- Identify and investigate anomalies
- Activate incident response process as necessary

Identify breach indicators

Phase 2

Network Breach Indicators

- Unusual…
  - …volume or type of network activity
  - …protocols, or protocols not being used properly
  - …files being downloaded
- Traffic associated with known “bad” hosts
- Traffic patterns associated with known malicious software

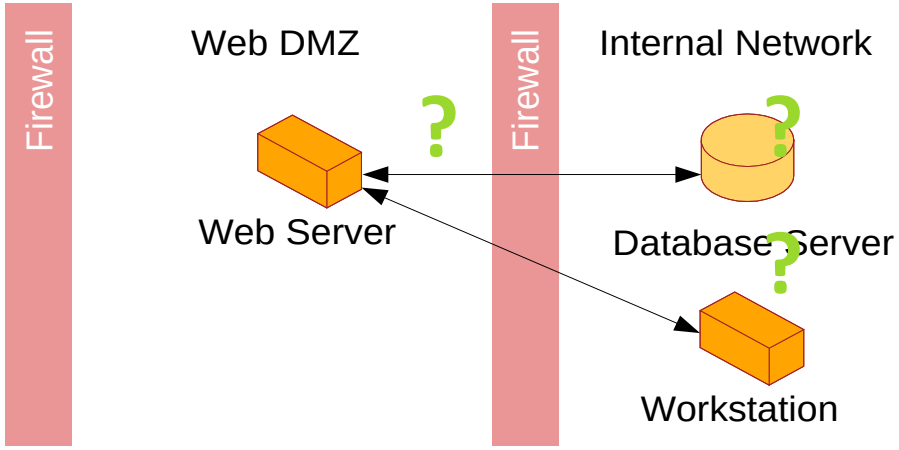


Identify breach indicators

Phase 2

System Breach Indicators

- Unusual…
  - …services
  - …registry keys
  - …files
  - …network connections
- Unusual log entries
- Antivirus logs indicate malware detection



Identify breach indicators

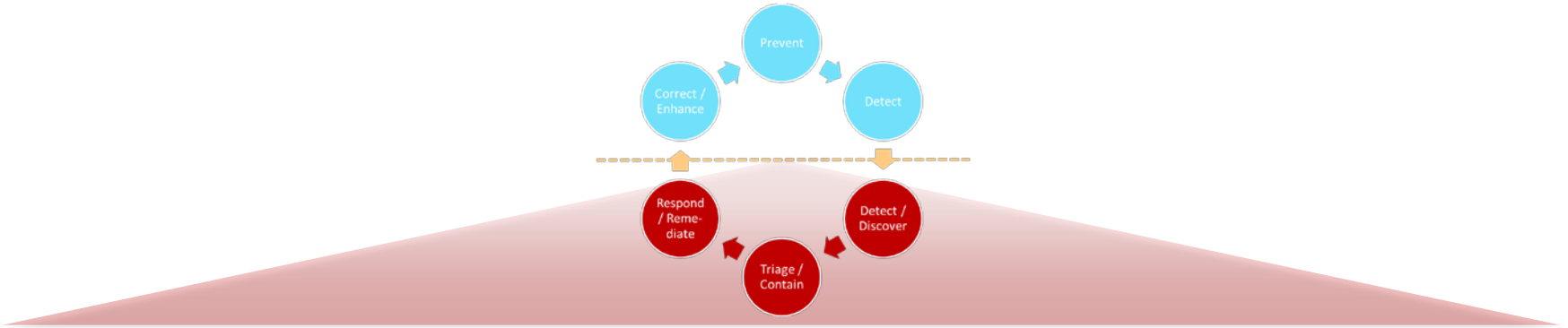
Phase 3

Evaluate susceptibility to future attacks

- Review findings to identify security vulnerabilities
- Execute threat-based scenario testing
- “Table top” exercises
- Revise operational processes to detect breach indicators
- Update your incident response plan based on lessons learned
- Determine baseline expectations

Incremental capabilities needed

Incremental solutions and capabilities



Organization & Governance	Information asset centric security	Threat Intelligence	Detection / Monitoring	Security behaviours & culture	Security in the business ecosystem	Incident response & crisis mgmt
Information Risk led approach along with effective governance	Clear view of what data exists & what is important. Information governance policy and program	Capability to understand and adapt security posture to emerging threats	Predictive monitoring / analytics bringing together multiple data sources.	People behave differently through clear grasp of what matters	Third party and supplier security management including data in the cloud	Integrated capability to respond to incidents
Preventative controls and IT Hygiene						

Source: PwC UK Cyber Threat Landscape April 2013

Organization & Governance

- Active board involvement
- Dedicated leadership for Information Security
- Clearly defined roles and responsibilities
- Skilled / knowledgeable resources for Incident Management Team
- On-going monitoring of control effectiveness
- Appropriate accountability
- Including all of the relevant stakeholders in security conversations (i.e., steering committee)

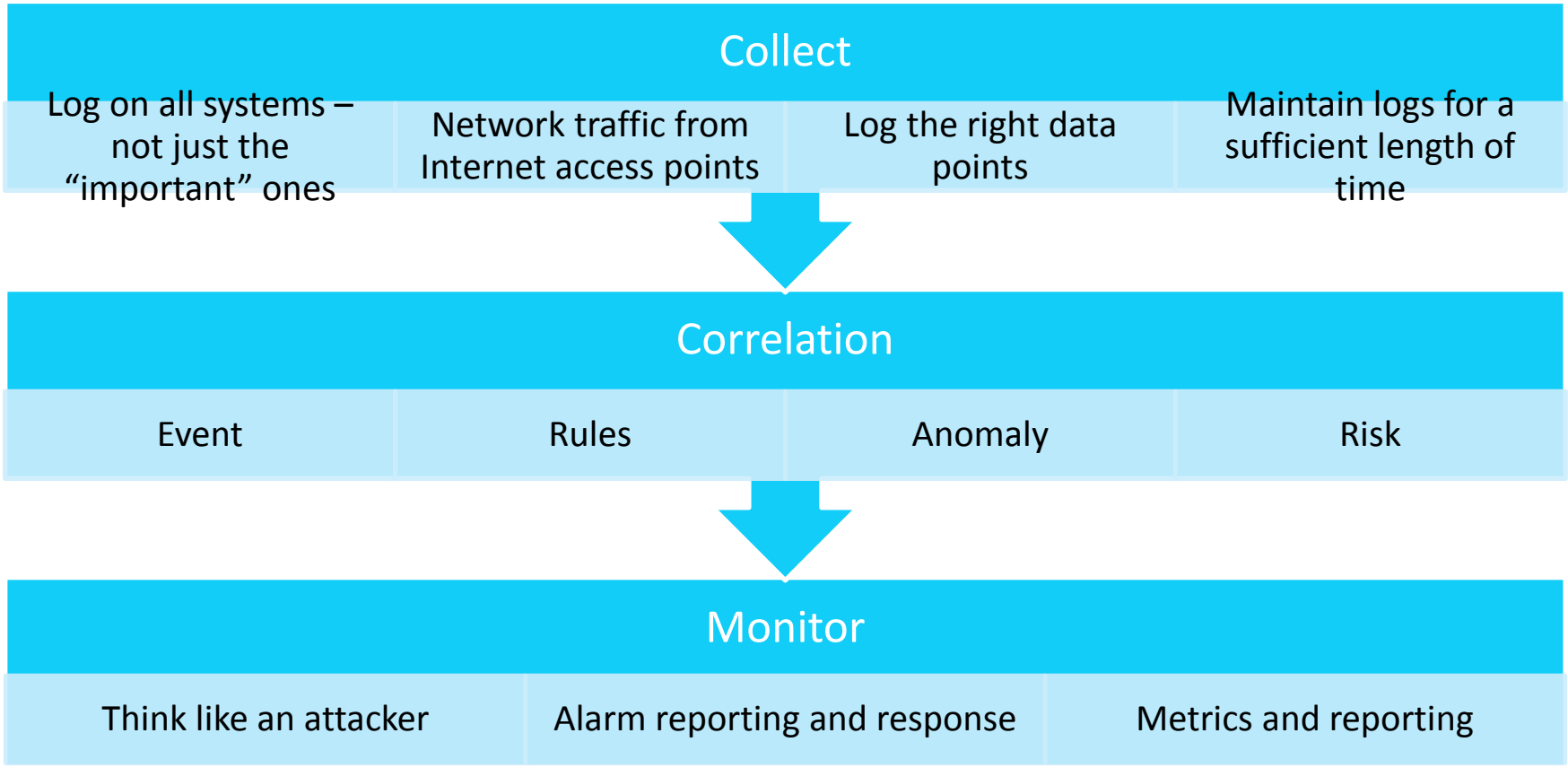
Information asset centric security

- Understand what data may be valuable and how it can be accessed
- Limit access to what is truly required
- Enhance monitoring to include data / business logic considerations
- Tie between identity management, logging, and data loss prevention technologies
- Segment disparate security zones

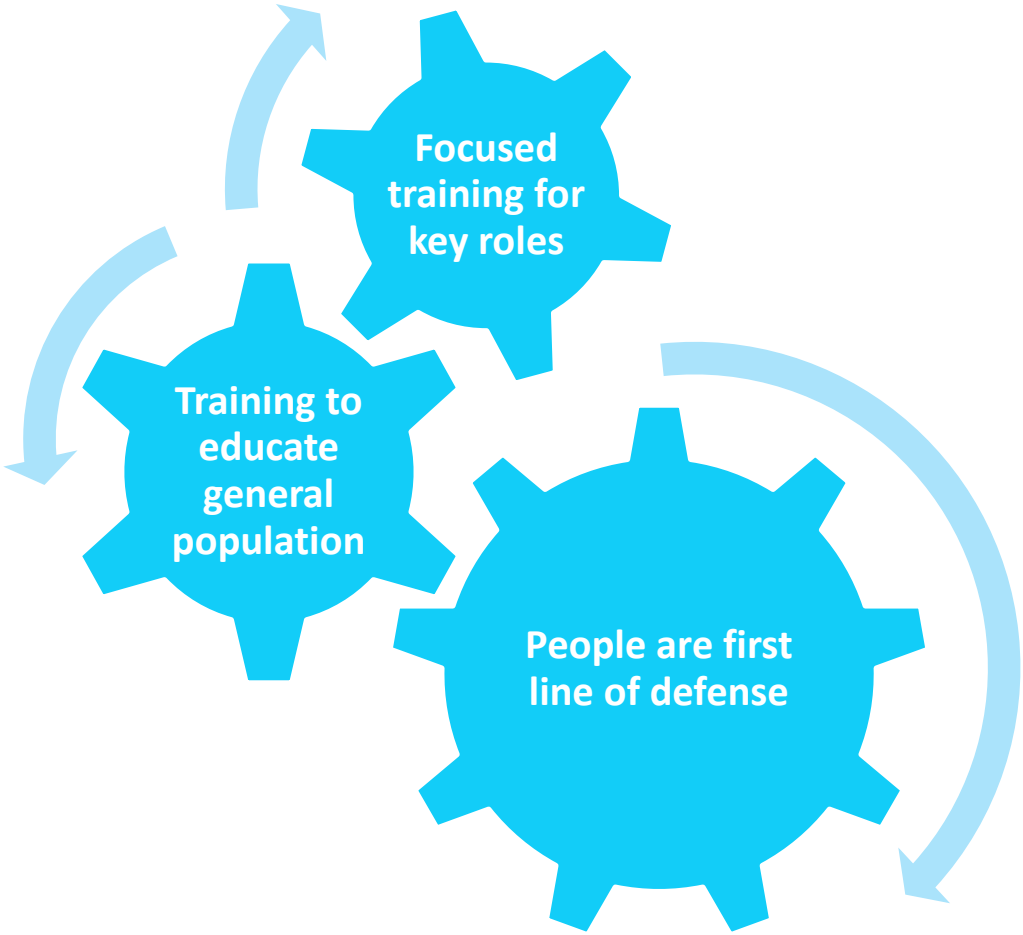
Threat intelligence

- Leverage business knowledge to enhance correlation rules
- Review intelligence from government agencies, for-profit vendors, and free sources
- Check with third parties to see if private IP address space is part of a known botnet or other cyber threat
- Analyze, spam, phishing and public disclosures
- Tie to law enforcement, industry groups and other sources
- Monitor social media

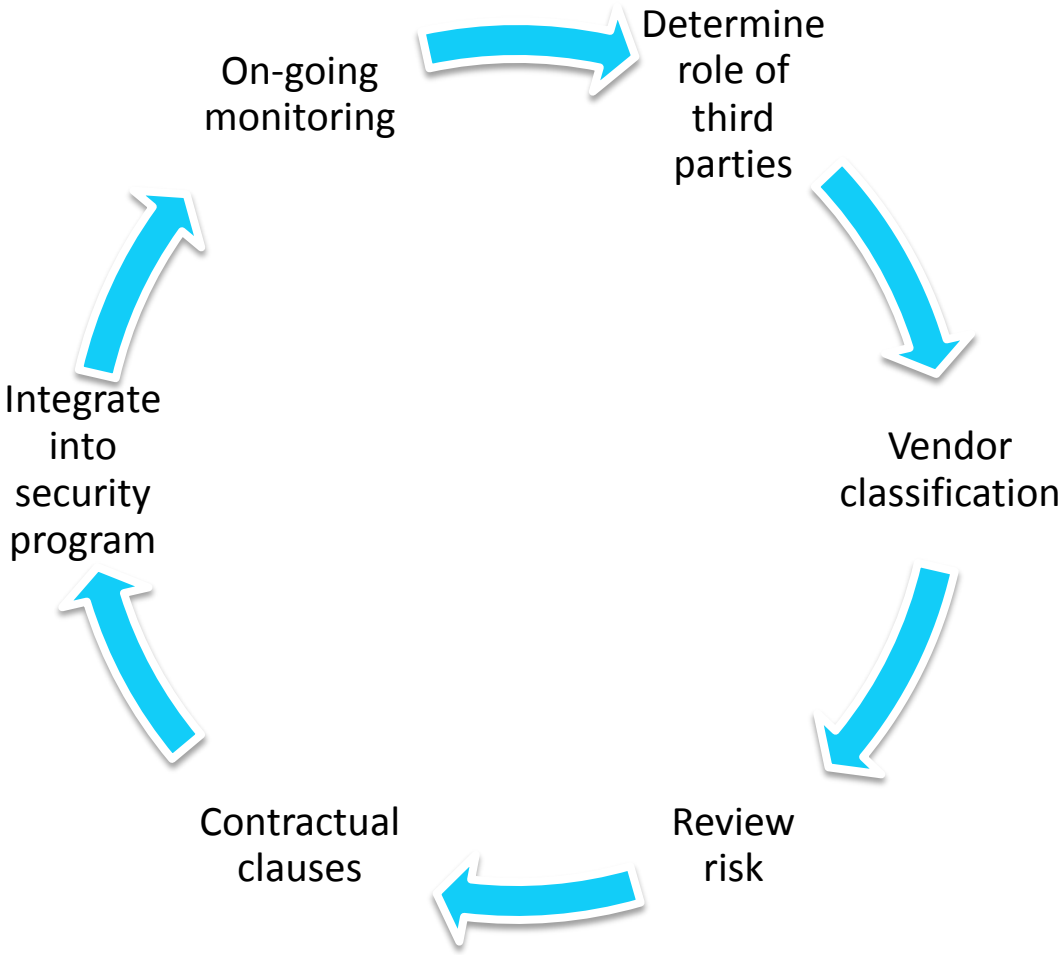
Detection / Monitoring



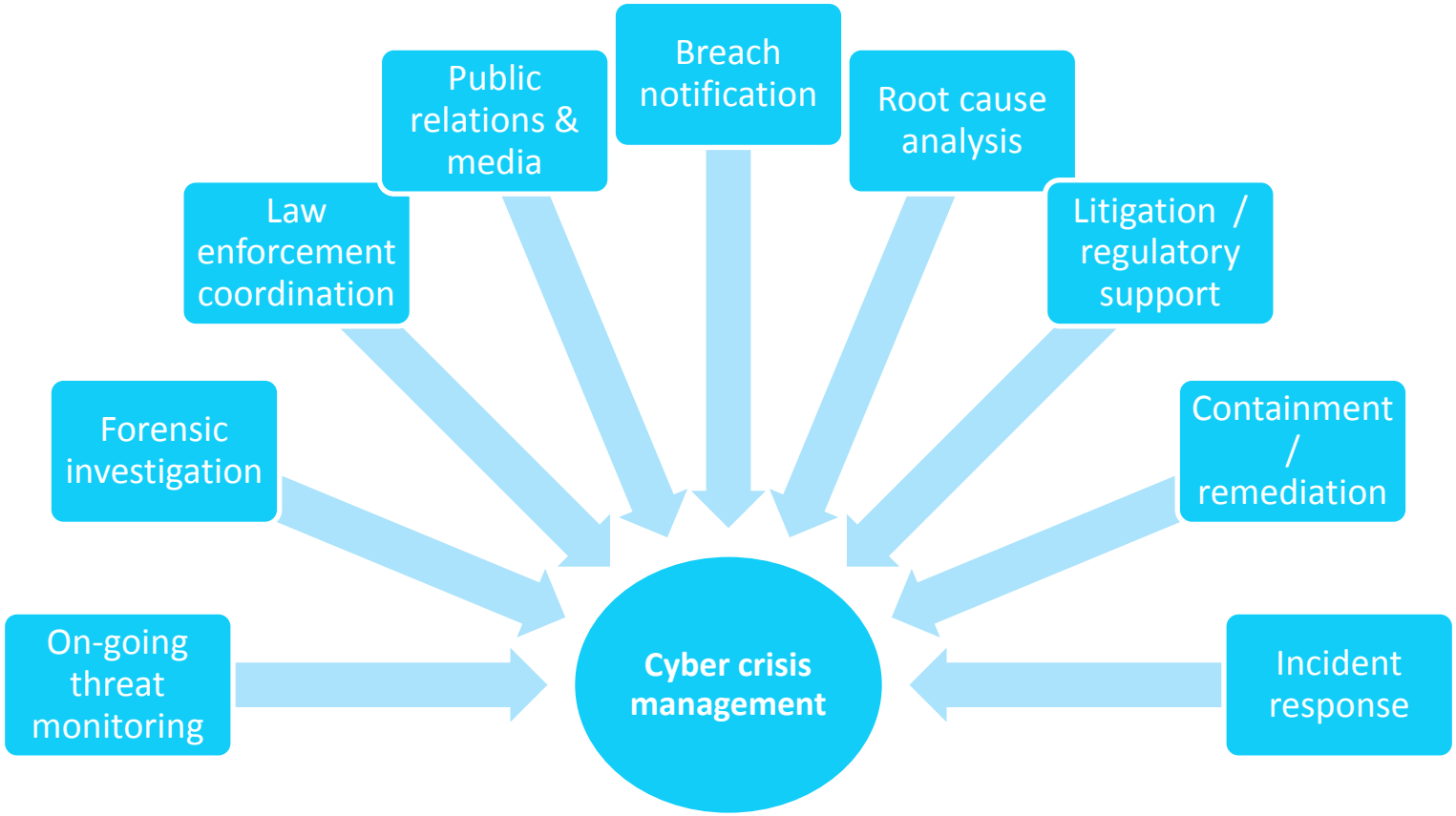
Security behaviors & culture



Security in the business ecosystem



Incident response & crisis management



Case studies of actual incidents

Financial services

Client issue:

- Cyber attack threat. Our client was notified by law enforcement that a cyber attack was imminent and likely to occur within 48 hours.
- Network intrusion. The client's external-facing systems were in danger of being breached, permitting access to back-end systems on the private network.
- Data theft and privacy breach. Payment card data and personally identifiable information were stored.

Outcome

- Network forensics. Analysis of historical network utilization data and identified the date of a mass data exfiltration.
- Data discovery. Determined the storage locations of data that might interest attackers to help focus the investigation and its security enhancement efforts.
- Breach indicator assessment identified more than 500 indicators of compromise.
- Live memory forensics. Preserved and analyzed volatile memory on systems it found that had indicators of malicious activity.
- Computer forensics. Forensically preserved and analyzed relevant systems and discovered previously undetected malware that had been installed nearly three years earlier.
- Malware analysis. The malware discovered had been permitting remote access to the client's private cyber space.

Financial services

Client issue:

- Global ATM fraud. ATM cards were counterfeited and then used to withdraw millions of dollars across the globe. The track data used to counterfeit the ATM cards came from our client's IT infrastructure.
- Malware. Unauthorized custom software was installed on internal systems, permitting remote access, querying of databases containing identities and payment card data, and collection of data flowing through the network.
- Data theft. Payment card data was collected and exfiltrated to external hosts without detection.

Outcome

- Computer forensics. The forensic analysis identified the initial point of intrusion and root cause, which systems had been compromised, malware installed on dozens of systems, and the how/where of undetected data exfiltration.
- Malware analysis. Twelve unprecedented malware instances, unknown and undetected by anti-virus technology, were discovered and analysed.
- Network forensics. Collected network traffic, and analyzed collected traffic for indicators of malicious activity. PwC also analyzed historical network utilization data and identified the date of a mass data exfiltration.
- Data discovery. To support the client's effort to determine the location of all data stores containing identity information, PwC launched its proprietary data discovery methodology which helped the client quantify the number of potentially exposed identities that would require privacy breach notification.

Questions?

Leonard Levy

leonard.l.levy@sg.pwc.com

+65 8571 3682

pwc