Cyber Security: An Internal Audit Perspective

By

Eoin Hayes

Senior Manager – Technology and Cyber
Group Internal Audit
Insurance Australia Group (IAG)
Sydney, Australia

Agenda

2.00-3.30

- Insurance Australia Group (IAG) Overview
- Overview of Cyber Security
- A brief history of Technology
- The Threat Landscape
- Cyber Security Standards & Frameworks

30 min Break

- Break Time will be from 3.30-4

4.00-4.30

- IAG Case Study: IA becoming a Trusted Advisor to the CISO
- Q&A (including questions from our online app)
- Security Awareness (2 x videos)
- Summary of Key Points

Audience Participation – our app!

Please use Sli.do app to ask questions throughout

We will have some polls for you to vote on also!

sli.do

How to log on – 2 ways:

1. Go to Slido.com. Put in code #Cyber

OR

2. Via your browser go to:
    - https://app.sli.do/event/pi2d9djy

iag

WE HAVE OVER

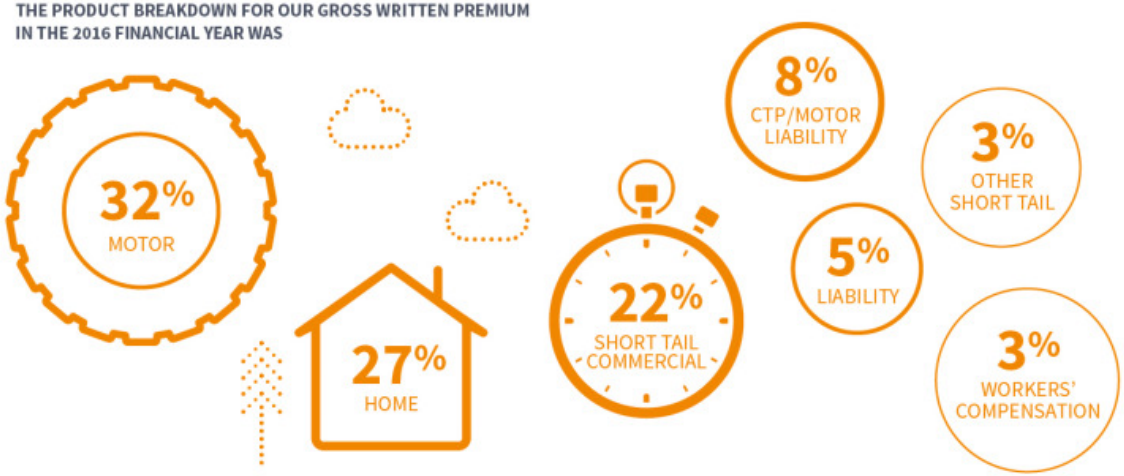
15,000

EMPLOYEES

IN THE 2016 FINANCIAL YEAR, WE INSURED AROUND

- FARMS 120,000
- EMPLOYERS 133,000
- HOMES 3.8 million
- CARS 8.0 million
- BUSINESSES 1.3 million

THE PRODUCT BREAKDOWN FOR OUR GROSS WRITTEN PREMIUM IN THE 2016 FINANCIAL YEAR WAS



OUR PORTFOLIO

AUSTRALIA

NRMA INSURANCE, SGIO, SGIC, swann insurance, RACV [1], CGU, wfi, coles Insurance [2]

NEW ZEALAND

STATE, NZI, ami, Lumley

VIETNAM

[3]

THAILAND

[4], NZI [4]

INDIA

SBIGeneral INSURANCE

MALAYSIA

[6] AmAssurance, KURNIA [6]

INDONESIA

ASURANSI PAROLAMAS [7]

100% owned unless marked with footnotes 1–7.

Cyber Security / Cyber Risk

Some definitions:

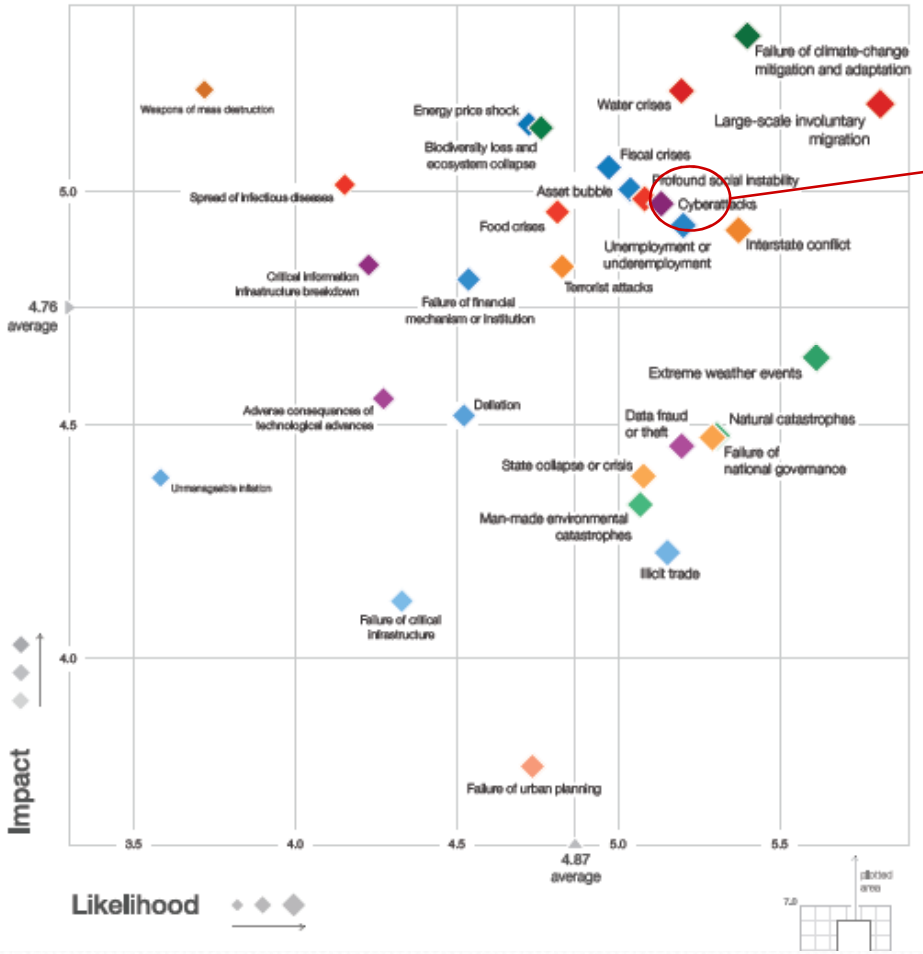
- "Cyber risk means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems (Institute of Risk Management)
- "Cyber risk can be defined as the risk connected to activity online, internet trading, electronic systems and technological networks, as well as storage of personal data" (PWC)

And Cyber Risk vs Cyber Security?

- Cybersecurity is the process of protecting information by preventing, detecting, and responding to attacks (NIST)

A Global Perspective

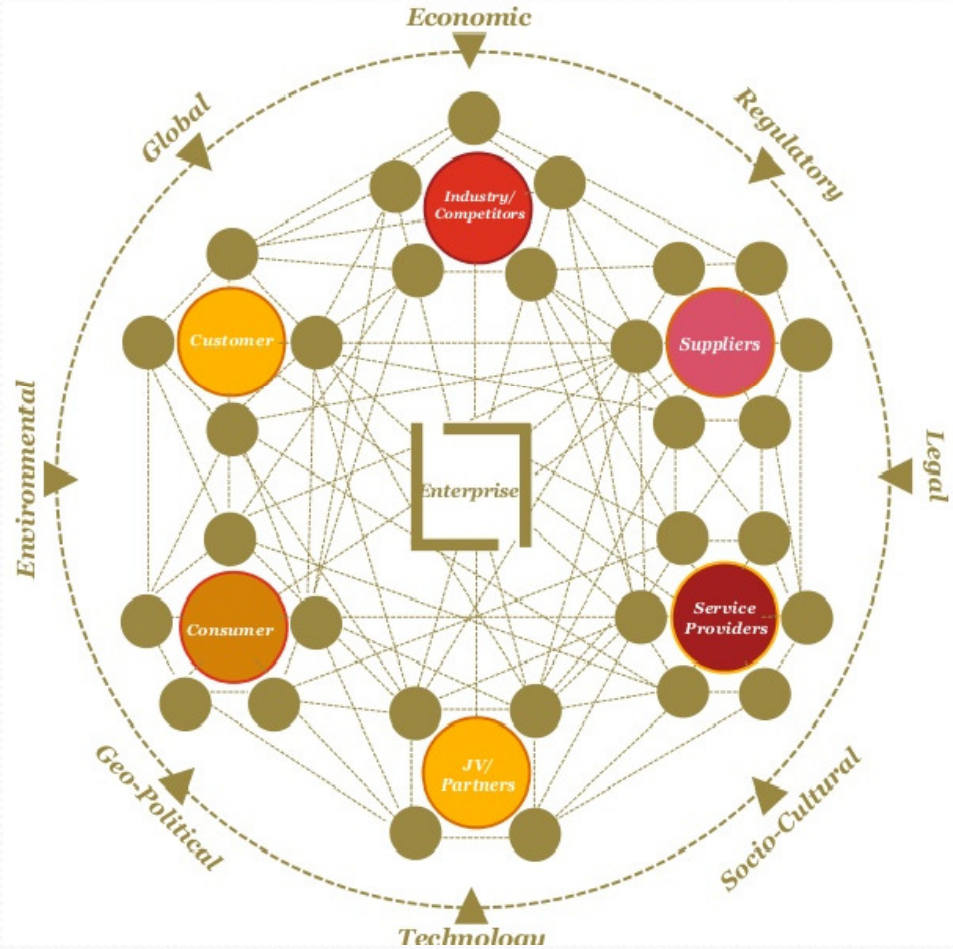
Figure 1: The Global Risks Landscape 2016



Cyber in the WEF's top right quadrant – high risk

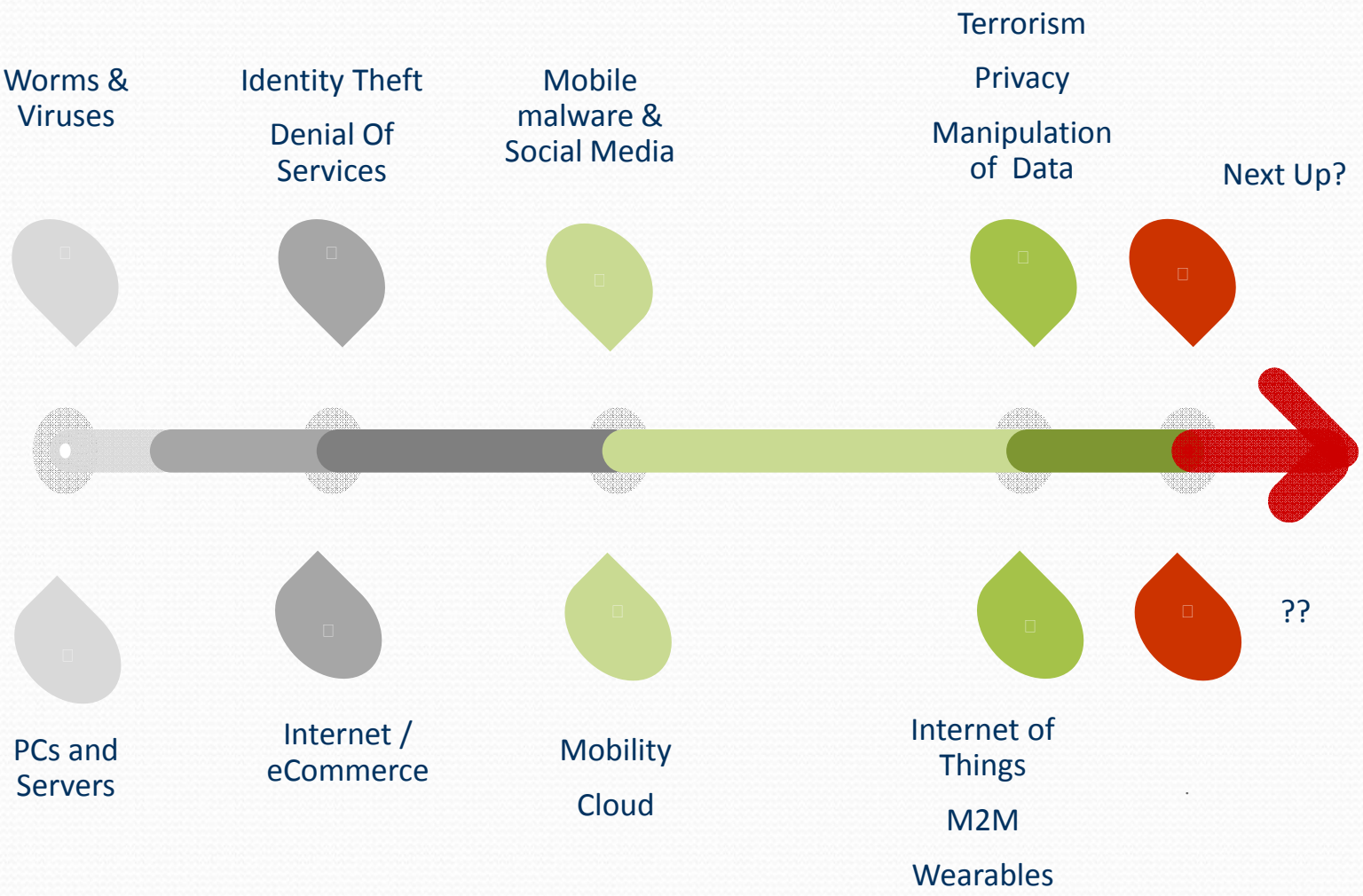
Source: World Economic Forum (WEF) Global Risk Report 2016

Everything is Connected



- **Technology is used by everyone** and every organisation
- Organisation are **inter-connected** in a complex web to a multitude of stakeholders
- Transactions transcend multiple parties, technologies and locations
- Built on **trust** and **collaboration**
- **COMPLEX!!**
- Gartner estimates 6.4 billion connected “things” in use today, up 30% from 2015…and will grow by more than 3 times, to nearly 21 billion by 2020

Evolution of Technology & Threats

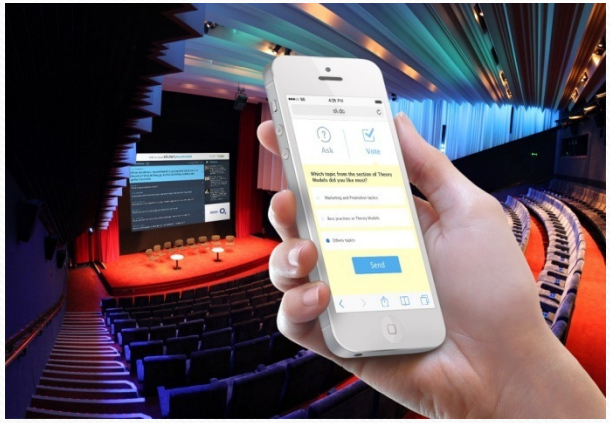


Some Big Threats about today

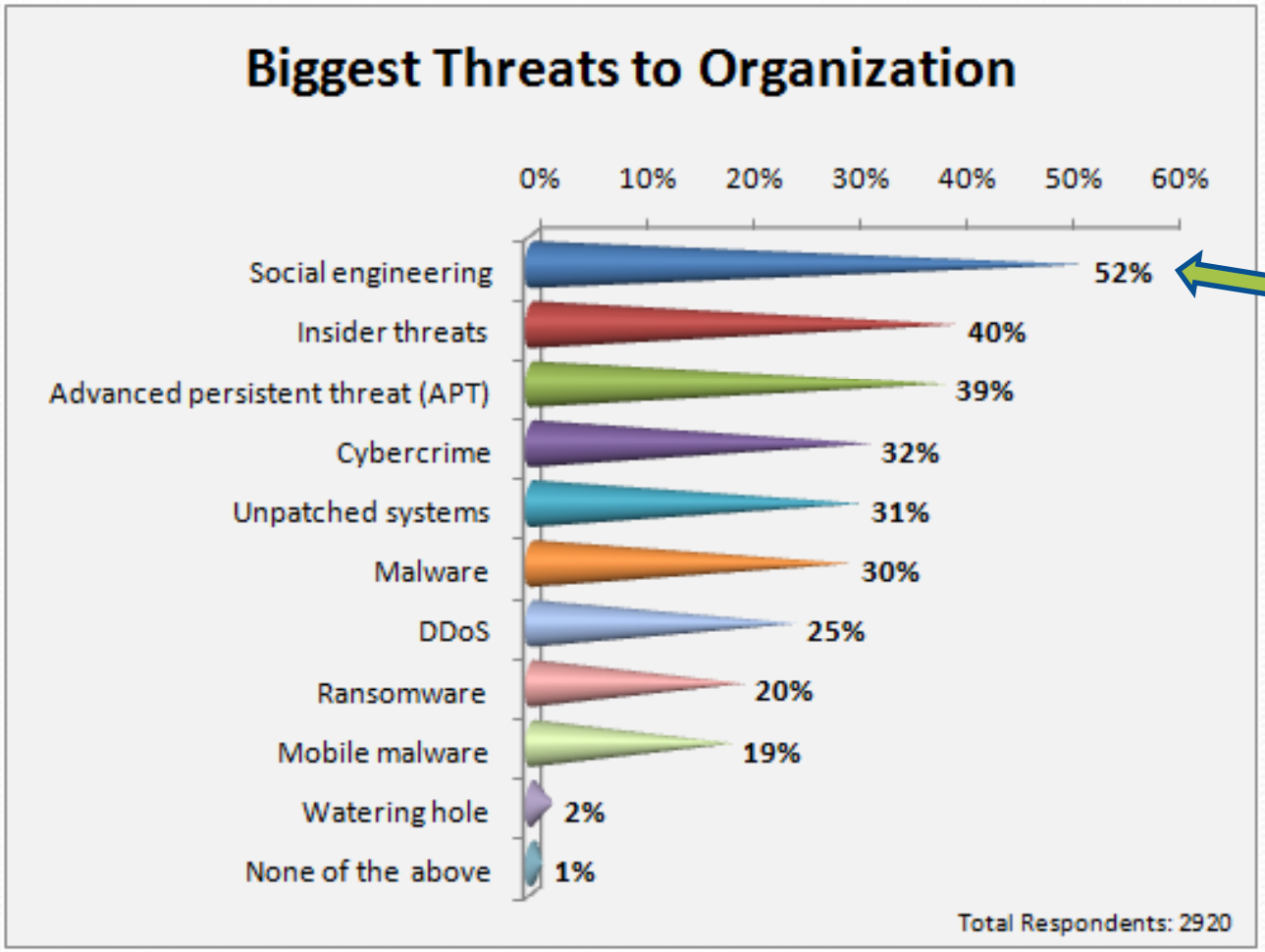
Threat	Description
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
Malware	Short for malicious software. Designed to infiltrate, damage or obtain information from a computer system.
Worm	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.
Social Engineering	An attack based on deceiving users or administrators at the target site into revealing confidential /sensitive information
APTs	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives using multiple attack vectors
DDoS	An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate
Watering Hole	In this attack, the attacker guesses or observes which websites a group (organization, industry, or region) often uses and infects one or more of them with malware.
Cybercrime	Cybercrime is defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offense
Unpatched systems	IT systems that do not have the most up to date known vulnerabilities addressed through applying available fixes/updates
Insider threat	Internal employee with access to sensitive /confidential data or systems that can cause damage either for personal gain or due to being disgruntled

Audience Participation!

Voting with your mobile – please choose the top threat you think your organisation faces today



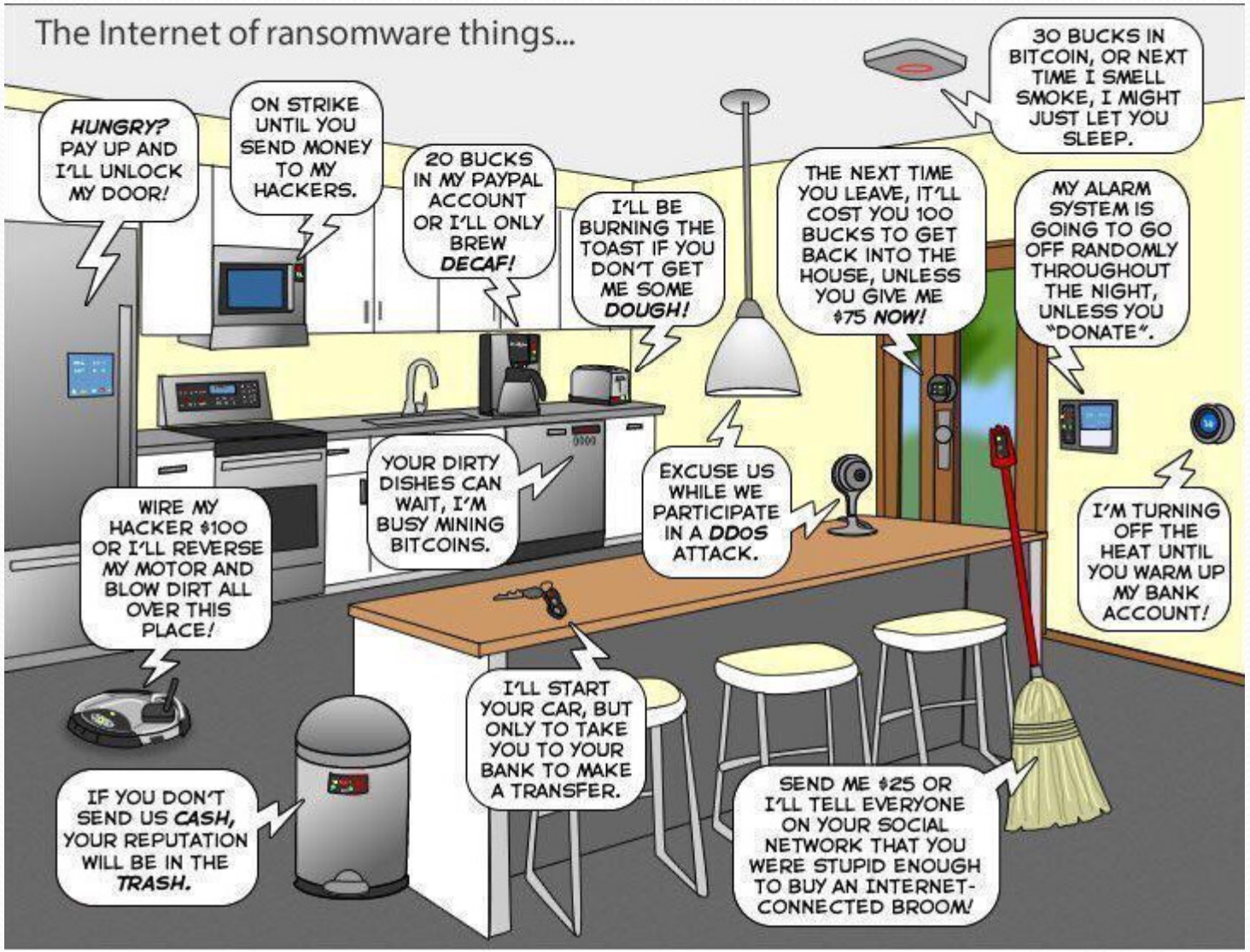
Threats in 2016



People are the weakest link

Source: ISACA Survey 2016

Cyber risks in the (near) future?



Who are we protecting from?

Nation States

MOTIVE: Economic, political, and/or military advantage

TARGET: Trade secrets • Sensitive business information • Emerging technologies • Critical infrastructure

IMPACT: Loss of competitive advantage • Disruption to critical infrastructure

Organised Crime

MOTIVE: Immediate financial gain • Collect information for future financial gains

TARGET: Financial / Payment Systems • Personally Identifiable Information • Payment Card Information • Protected Health Information

IMPACT: Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence

Hacktivists

MOTIVE: Influence political and /or social change • Pressure business to change their practices

TARGET: Corporate secrets • Sensitive business information • Information related to key executives, employees, customers & business partners

IMPACT: Disruption of business activities • Brand and reputation • Loss of consumer confidence

Insiders

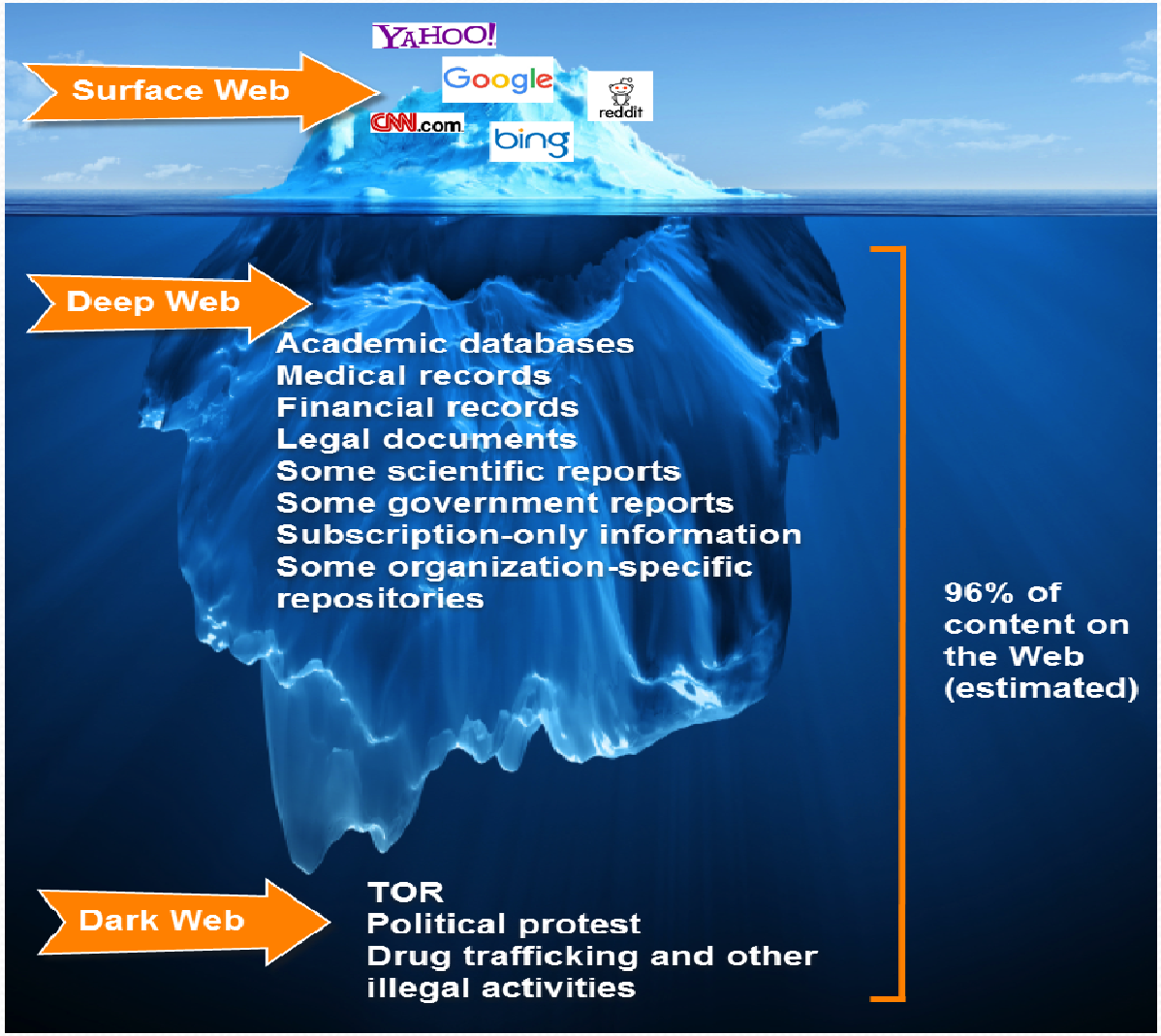
MOTIVE: Personal advantage, monetary gain • Professional revenge • Patriotism

TARGET: Sales, deals, market strategies • Corporate secrets, IP, R&D • Business operations • Personnel information

IMPACT: Trade secret disclosure • Operational disruption • Brand and reputation • National security impact

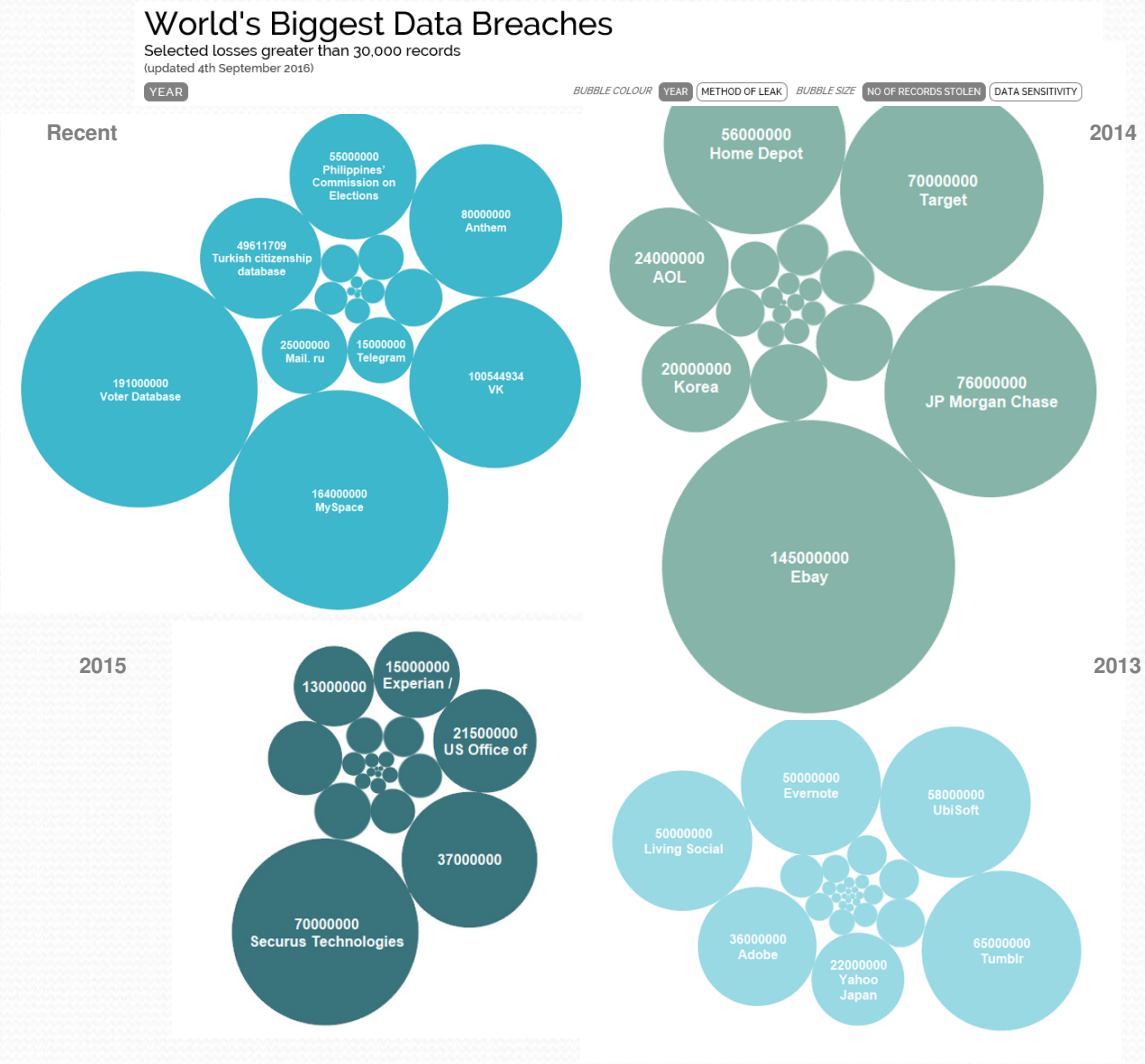
Source: PWC Global State of Information Security Survey 2016

Where do criminals interact?



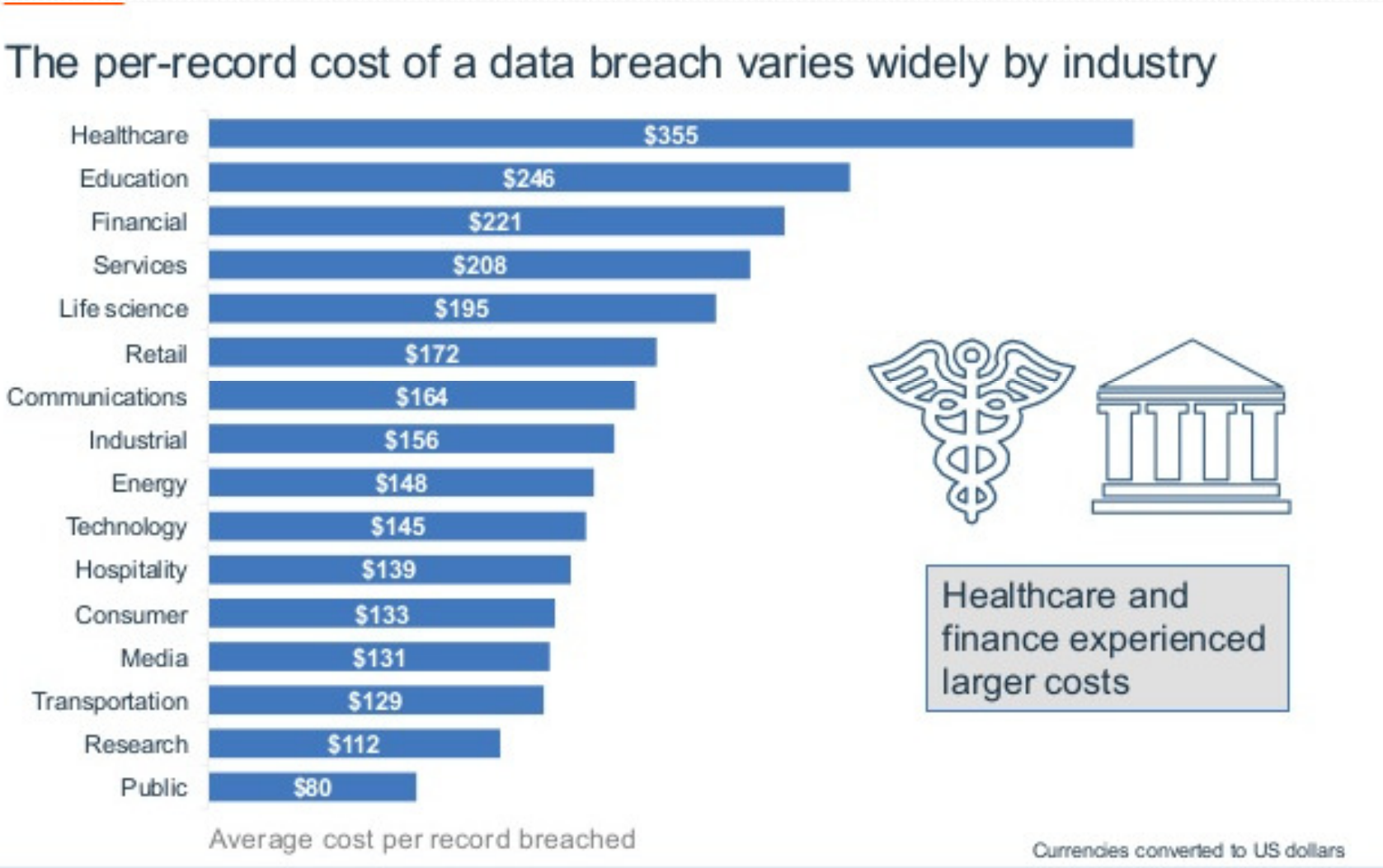
Some well known breaches

- Mossack Fonseca
- US Office of Personnel (2nd breach)
- AshleyMadison.com
- SONY
- Anthem
- JP Morgan
- LinkedIn
- DropBox
- Australian Immigration
- US Military
- UK Ministry of Defense
- Yahoo



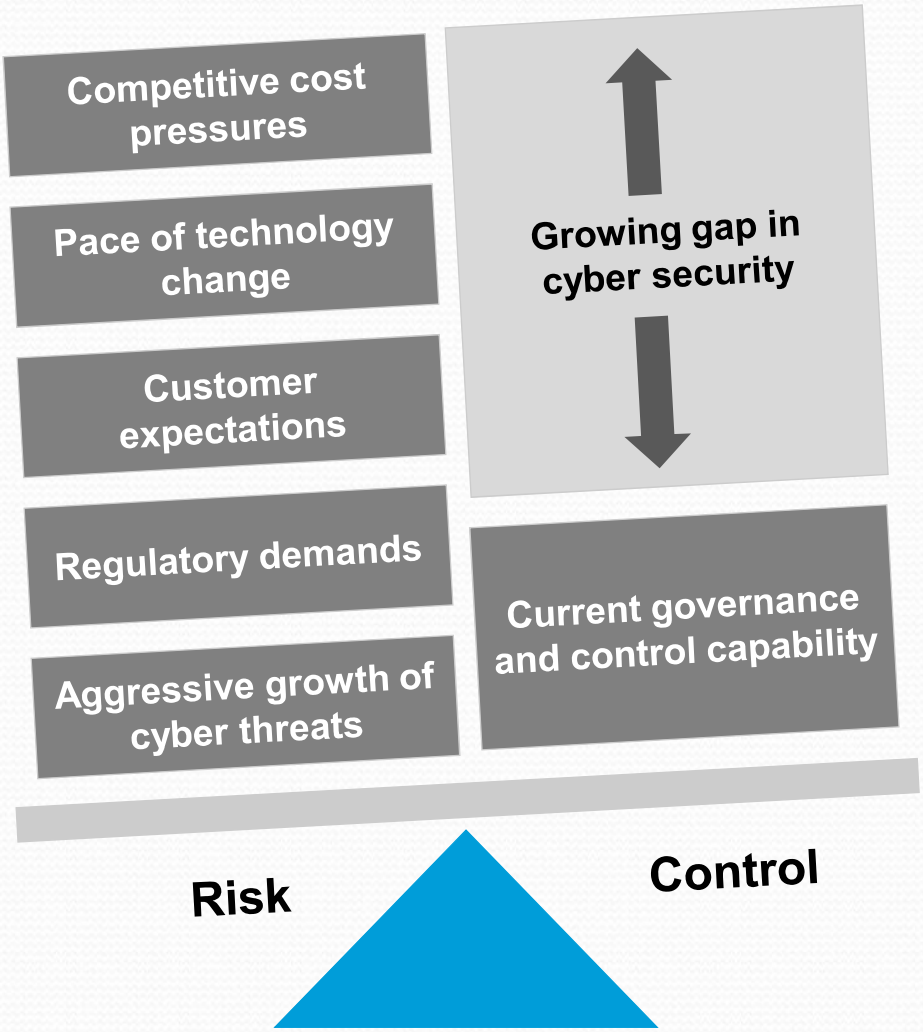
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

And some data is more valuable



Source: 2015 IBM & Ponemon Institute's Cost of Data Breach Study

The challenge for organisations today



- Technology driving significant changes in operations, exposing customer data via digital channels
- Extended supply chain – cyber criminals focus on weakest link
- Historic business models has meant existing security capability relatively immature – lack of skills
- Increased erosion of perimeter from third parties, social media, mobile and personal devices
- Growing regulatory focus
- Rising level and sophistication of external threat
- Cyber risk is outpacing organisations' ability to keep up

The response by organisations

52% have security baselines/standards for third parties

53% have an awareness and training program .

58% have an overall Information Security Strategy

54% Have a CISO in charge of security

49% Conduct threat assessments

48% Active monitoring / analysis of security intelligence

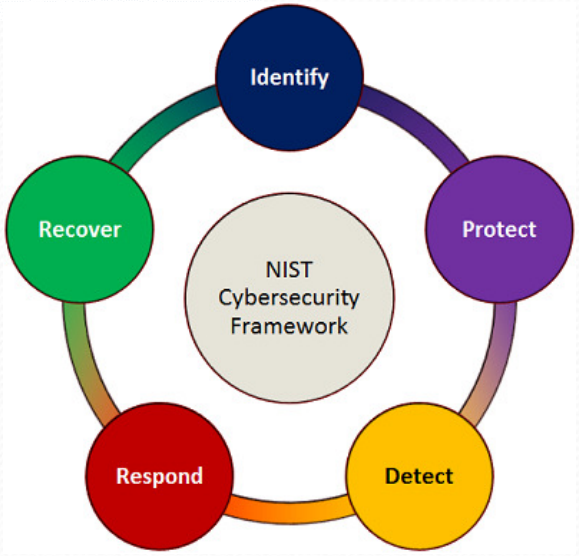
Businesses are investing in core safeguards to better defend their ecosystems against evolving threats

Source: PWC Global State of Information Security Survey 2016

Better practice security standards

ISO 27001

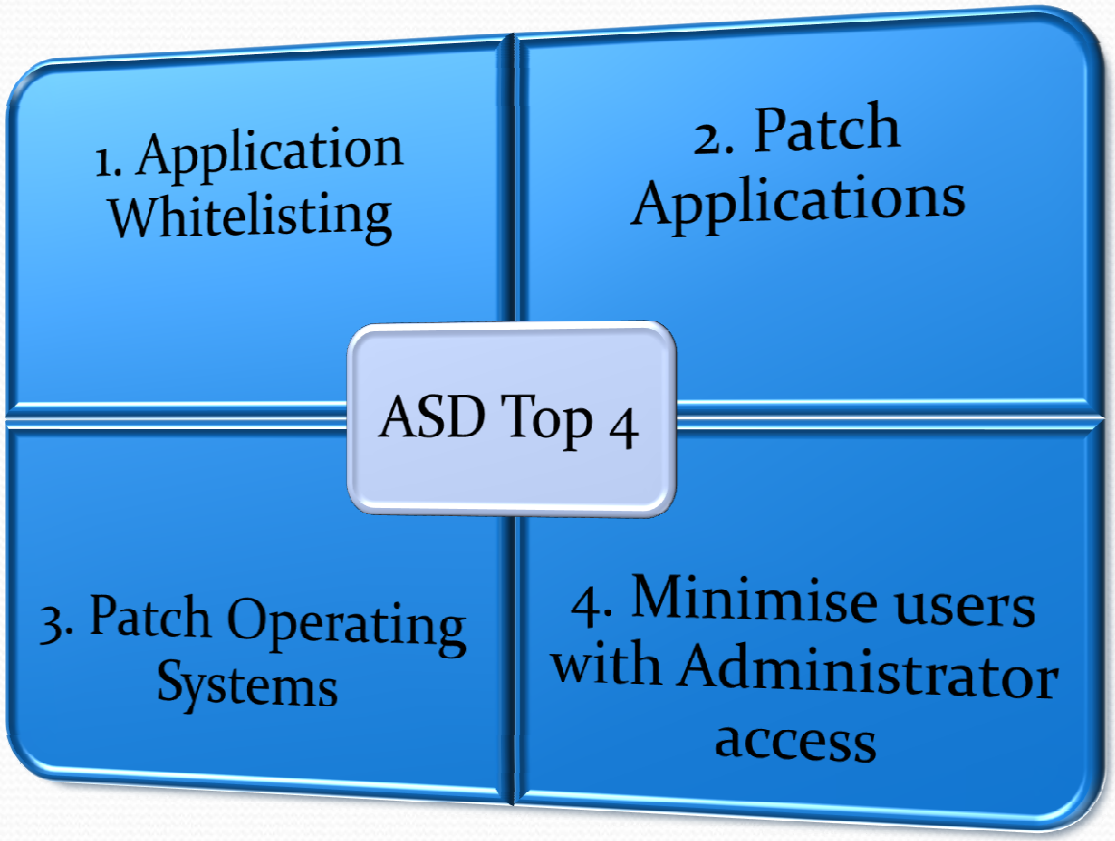
STRATEGIES to MITIGATE
TARGETED CYBER INTRUSIONS
ASD TOP 4 PREVENTS OVER 85% OF INTRUSIONS



SANS 20
CRITICAL SECURITY CONTROLS

ASD Top 4

Do this at a minimum – prevents 85% of threats – best "bang for your buck".



http://www.asd.gov.au/publications/protect/top_4_mitigations.htm

NIST Cybersecurity Framework

IDENTIFY

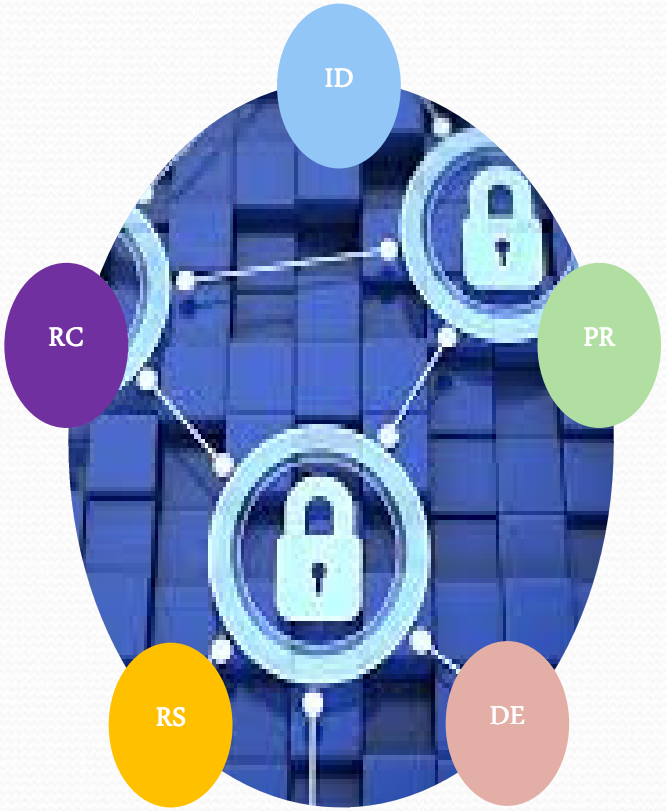
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities

PROTECT

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.



RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

https://www.nist.gov/cyberframework

IDENTIFY Control Categories

Framework

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

Function	Category Identifier	Category
IDENTIFY (ID)	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy

PROTECT Control Categories

Framework

- IDENTIFY
- **PROTECT**
- DETECT
- RESPOND
- RECOVER

Function	Category Identifier	Category
PROTECT (PR)	PR.AC	Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection Processes and Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology

DETECT Control Categories

Framework

- IDENTIFY
- PROTECT
- **DETECT**
- RESPOND
- RECOVER

Function	Category Identifier	Category
DETECT (DE)	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes

RESPOND Control Categories

Framework

- IDENTIFY
- PROTECT
- DETECT
- **RESPOND**
- RECOVER

Function	Category Identifier	Category
RESPOND (RS)	RS.RP	Response Planning
	RS.CO	Communications
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements

RECOVER Control Categories

Framework

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

Function	Category Identifier	Category
RECOVER (RC)	RC.RP	Recovery Planning
	RC.IM	Improvements
	RC.CO	Communications

- 15 minute break
- Please don’t forget to put up your questions using our voting app
- Review feed and “like” comments/questions to push them up the queue

Security Awareness Video (1)

Social Engineering in Action – promotion for Safe Internet Banking to raise awareness for customers

Movie Clip

What is Internal Audit's Role?

- Not solely a task for the Cyber Security team
- And also not just an IT issue – a business one also
- Internal audit have a unique position to look across the organisation and should use it in this area also
- IA can come in early when security strategies are being devised to
    - provide a second opinion;
    - Independently validate self-assessments; and
    - provide comfort to the Board and Audit Committee that investment is being directed to the right areas.

How best to approach this

Build initial relationship

- The CAE and CISO (Chief Information Security Officer) must first engage and understand each other's overall objectives, strategies and team capabilities

Build Trust

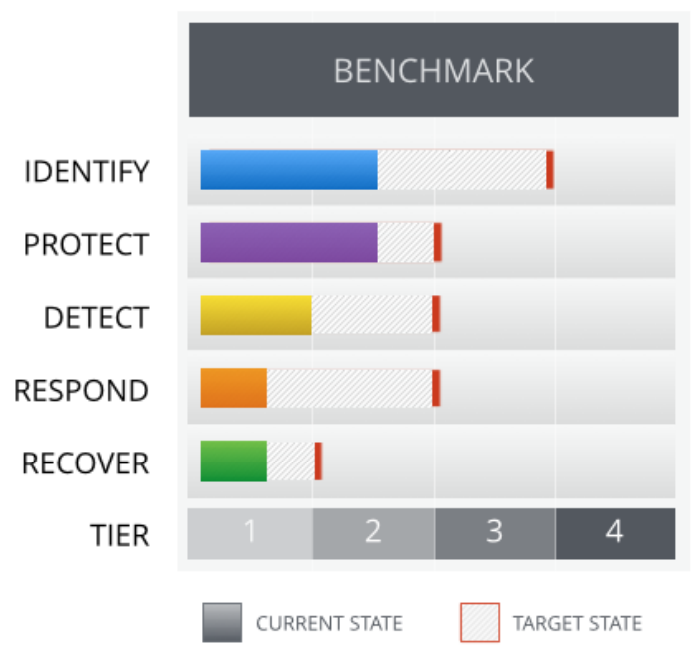
- *Subject Matter Expertise*: Having an internal audit resources and/or co-source partner with IT and cyber knowledge to engage with the CISO and team
- *Collaborate and share*: provide regular insights from other audits that may be of interest, use of external partners to provide industry insight
- *Align*: Use similar frameworks, benchmarks and language to avoid a mismatch and inconstant messaging to the board
- *Deliver*: Once planned, deliver your audits and reviews with a degree of professionalism with constant communication throughout to ensure the final result is value-add to all
- *Follow-up*: Develop an ongoing audit plan that aligns with the Cyber security plans
- *Continuous check in*: Keep the relationship going outside of audit time

How we approached it at IAG

- Internal Audit used the same NIST framework to assess to ensure consistency of language and messaging to the executives and board
- Assessed using the 5 domains of NIST – IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER
- Provided an independent view on maturity ratings and priority areas to uplift and invest in
- Provided a view on proposed security strategy to ensure priorities were focused in right areas
- Held several workshops to align and agree on findings and results
- Constant communication throughout the review to ensure the team and CISO were kept informed

Outputs

- An aligned view on the current security state and the strategy roadmap needed to achieve the desired target state
- Some of the challenges the strategy aimed to overcome were:
  - ❖ The importance of getting the fundamentals right
  - ❖ The need to enhance detection and response rather than just focus on protection
  - ❖ Ensuring Cybersecurity by design
  - ❖ Enhancing Cybersecurity awareness
- Results presented jointly to the Audit and Risk Committees to provide both the self-assessed and IA validated views on current, target states and roadmap



Benefits

- Board gained comfort that investment was being directed in the right areas – those that will reduce risk the most
- Internal audit cyber plan linked with the cyber security roadmap with regular "health checks" integrated into overall security plan
- IA and Cyber Security had a very good relationship with understanding of when and how IA can provide value – ***A TRUSTED ADVISOR***

Understanding & Awareness

Becoming a Trusted Cyber Advisor is not just about…

- Knowing the basic concepts of cyber
- Collaborating with the security team only
- Relying solely on IT staff to provide cyber security expertise

It is also…

✓ Expanding IT audit capabilities to provide proactive, actionable insights

✓ Maintaining a strong working knowledge of upcoming changes in regulation, new insurance coverage requirements, new class-action lawsuits, and other trends.

✓ Ensuring that audit programs consider these trends

✓ Ensuring cybersecurity competencies for the CAE and staff through effective talent management/professional development programs

✓ Strategically leveraging co-sourcing to ensure the right talent and competence is available as needed

Risk Management

Becoming a Trusted Cyber Advisor is not just about…

- Conducting a risk assessment to determine the likelihood + impact of cyber risks
- Being aware of how the organization addresses cybersecurity and the actions management has taken to mitigate related risks
- Reviewing third-party audit reports

It is also…

- ✓ Staying abreast with the frequency and magnitude of cybersecurity lapses
- ✓ Understanding full impact of cyber threats on the organization and embedding this in the audit plan
- ✓ Proactively identifying emerging cybersecurity risks
- ✓ Understanding the organization's risk posture to combat cyber threats
- ✓ Performing continuous auditing on management's cybersecurity controls
- ✓ Partnering with the CIO/CISO to assess third-party candidates
- ✓ Contributing to third-party candidate risk profiles
- ✓ Advising on third-party compatibility with the cyber security strategy/philosophy

Assurance

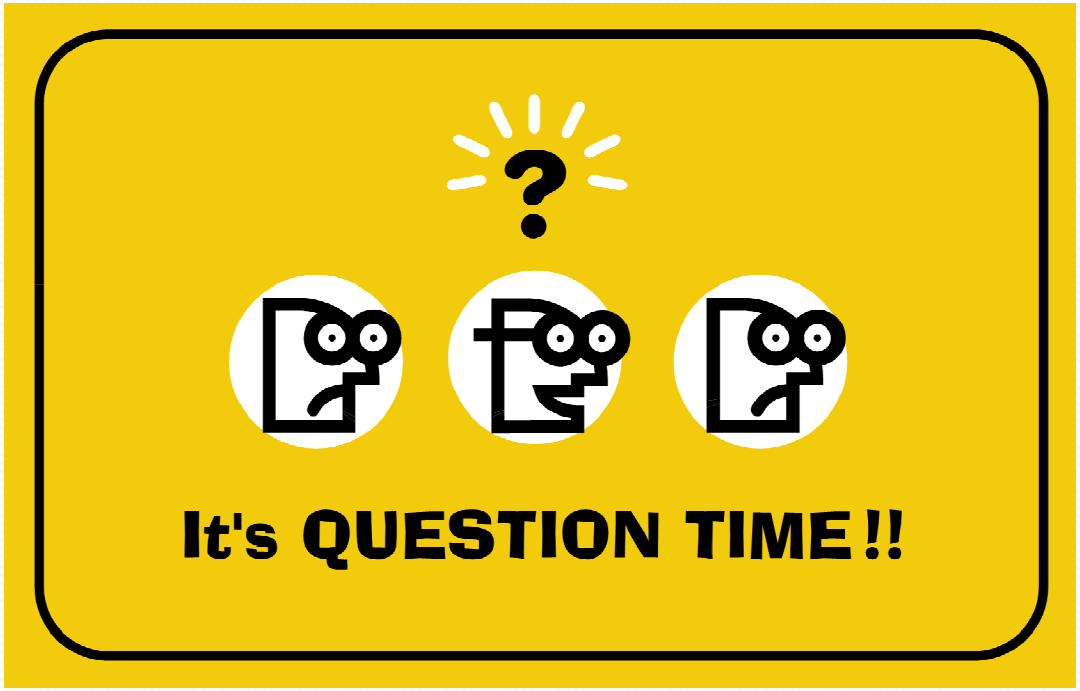
Becoming a Trusted Cyber Advisor is not just about…

- Assessing compliance with cyber-related policies and procedures
- Providing assurance on the organization's cybersecurity program
- Providing assurance on incident response, disaster recovery, and business continuity plans
- Reporting cybersecurity-related engagement results to management and board/audit committee

It is also…

- ✓ An independent review of the cybersecurity strategy before the policies & procedures are developed
- ✓ Being part of technology project implementation teams to ensure cyber risks are addressed and built-in, rather than added on later
- ✓ Benchmarking & testing the adequacy and effectiveness of policies/procedures against applicable frameworks
- ✓ Evaluating training outcomes and knowledge retention
- ✓ Leveraging internal audit capabilities with existing bench strength in 1st/2nd lines of defence
- ✓ Providing insights on the coordination of plans and alignment with business strategy
- ✓ Engaging management and the board/audit committee in forward-looking discussions, helping them to think through the cyber vulnerabilities facing the organization

Top questions from our app



Security Awareness Video (2)

- Cyber Threat and Response – (Symantec / Deloitte collaboration)
- What an real-life attack looks like and what a speedy response should entail
- Incident Response is a key control in cyber security – you can't prevent everything so when an attack occurs you need to be prepared!

Movie Clip

Key Takeaways

- Cyber Risk – a focus right up to Board level these days

The Board

- Technology is ever evolving making us more and more connected - but this comes with ever evolving threats also

Evolving Threats

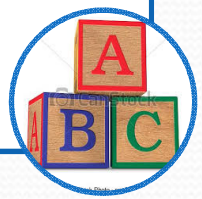
- Organisations need to up their levels of security controls to combat this

Uplift Security

Key Takeaways

- Focus on the fundamentals first

The Basics



- Biggest challenge is not technology but people – need to build awareness

People

- Response and Recovery is as important (if not more) than Prevention

Response

Key Takeaways

- Lots of Standards and Frameworks to measure your organisation against

Measure

- Audit can add value by working collaboratively with Cyber Security as they develop their strategies; using common language & frameworks to avoid confusion e.g. NIST

Collaborate

- Cyber Risk is continuously evolving so Internal Audit must have a continuous and responsive approach to assurance over it…to become a true trusted advisor.

Trusted Advisor