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!

**How to log on – 2 ways:**

1. Go to Slido.com. Put in code #Cyber
2. Via your browser go to:
   - [https://app.sli.do/event/pi2d9djy](https://app.sli.do/event/pi2d9djy)
WE HAVE OVER 15,000 EMPLOYEES

IN THE 2016 FINANCIAL YEAR, WE INSURED AROUND

<table>
<thead>
<tr>
<th>Category</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farms</td>
<td>120,000</td>
</tr>
<tr>
<td>Employers</td>
<td>133,000</td>
</tr>
<tr>
<td>Homes</td>
<td>3.8 million</td>
</tr>
<tr>
<td>Cars</td>
<td>8.0 million</td>
</tr>
<tr>
<td>Businesses</td>
<td>1.1 million</td>
</tr>
</tbody>
</table>

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

- 32% Motor
- 27% Home
- 22% Short Tail Commercial
- 8% CTP/Motor Liability
- 3% Other Short Tail
- 5% Liability
- 3% Workers’ Compensation

OUR PORTFOLIO

AUSTRALIA

NEW ZEALAND

VIETNAM

THAILAND

INDIA

MALAYSIA

INDONESIA

100% owned unless marked with footnotes 1-7.
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)
Figure 1: The Global Risks Landscape 2016

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

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

- Worms & Viruses
- Identity Theft
  - Denial Of Services
- Mobile malware & Social Media
- Terrorism
  - Privacy
  - Manipulation of Data
- Next Up?
- PCs and Servers
- Internet / eCommerce
- Mobility Cloud
- Internet of Things
  - M2M
  - Wearables
- ??
### Some Big Threats about today

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ransomware</strong></td>
<td>A type of malicious software designed to block access to a computer system until a sum of money is paid.</td>
</tr>
<tr>
<td><strong>Malware</strong></td>
<td>Short for malicious software. Designed to infiltrate, damage or obtain information from a computer system.</td>
</tr>
<tr>
<td><strong>Worm</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Social Engineering</strong></td>
<td>An attack based on deceiving users or administrators at the target site into revealing confidential/sensitive information</td>
</tr>
<tr>
<td><strong>APTs</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>DDoS</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Watering Hole</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Cybercrime</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Unpatched systems</strong></td>
<td>IT systems that do not have the most up to date known vulnerabilities addressed through applying available fixes/updates</td>
</tr>
<tr>
<td><strong>Insider threat</strong></td>
<td>Internal employee with access to sensitive/confidential data or systems that can cause damage either for personal gain or due to being disgruntled</td>
</tr>
</tbody>
</table>
Audience Participation!

Voting with your mobile – please choose the top threat you think your organisation faces today
People are the weakest link

Threats in 2016

Source: ISACA Survey 2016
Cyber risks in the (near) future?

The Internet of ransomware things...

- Hungry? Pay up and I’ll unlock my door!
- On strike until you send money to my hackers.
- 20 bucks in my PayPal account or I’ll only brew decaf!
- I’ll be burning the toast if you don’t get me some dough!
- The next time you leave, it’ll cost you 100 bucks to get back into the house, unless you give me $75 now!
- 30 bucks in Bitcoin, or next time I smell smoke, I might just let you sleep.
- Wire my hacker $100 or I’ll reverse my motor and blow dirt all over this place.
- Your dirty dishes can wait, I’m busy mining bitcoins.
- Excuse us while we participate in a DDoS attack.
- I’ll start your car, but only to take you to your bank to make a transfer.
- Send me $25 or I’ll tell everyone on your social network that you were stupid enough to buy an internet-connected broom.
- My alarm system is going to go off randomly throughout the night, unless you “donate”.
- I’m turning off the heat until you warm up my bank account.
- If you don’t send us cash, your reputation will be in the trash.
<table>
<thead>
<tr>
<th>Group</th>
<th>Motive</th>
<th>Target</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation States</td>
<td>Economic, political, and/or military advantage</td>
<td>Trade secrets • Sensitive business information • Emerging technologies • Critical infrastructure</td>
<td>Loss of competitive advantage • Disruption to critical infrastructure</td>
</tr>
<tr>
<td>Organised Crime</td>
<td>Immediate financial gain • Collect information for future financial gains</td>
<td>Financial / Payment Systems • Personally Identifiable Information • Payment Card Information • Protected Health Information</td>
<td>Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Influence political and /or social change • Pressure business to change their practices</td>
<td>Corporate secrets • Sensitive business information • Information related to key executives, employees, customers &amp; business partners</td>
<td>Disruption of business activities • Brand and reputation • Loss of consumer confidence</td>
</tr>
<tr>
<td>Insiders</td>
<td>Personal advantage, monetary gain • Professional revenge • Patriotism</td>
<td>Sales, deals, market strategies • Corporate secrets, IP, R&amp;D • Business operations • Personnel information</td>
<td>Trade secret disclosure • Operational disruption • Brand and reputation • National security impact</td>
</tr>
</tbody>
</table>

Where do criminals interact?

Surface Web
- Yahoo!
- Google
- CNN.com
- Bing

Deep Web
- Academic databases
- Medical records
- Financial records
- Legal documents
- Some scientific reports
- Some government reports
- Subscription-only information
- Some organization-specific repositories

Dark Web
- TOR
- Political protest
- Drug trafficking and other illegal activities

96% of content on the Web (estimated)
Some well known breaches

- Mossack Fonseca
- US Office of Personnel (2\textsuperscript{nd} 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

The per-record cost of a data breach varies widely by industry:

- Healthcare: $355
- Education: $246
- Financial: $221
- Services: $208
- Life science: $195
- Retail: $172
- Communications: $164
- Industrial: $156
- Energy: $148
- Technology: $145
- Hospitality: $139
- Consumer: $133
- Media: $131
- Transportation: $129
- Research: $112
- Public: $80

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

Better practice security standards

ISO 27001

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

NIST Cybersecurity Framework

IDENTIFY
PROTECT
RECOVER
RESPOND

SANS 20 CRITICAL SECURITY CONTROLS
ASD Top 4

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

1. Application Whitelisting
2. Patch Applications
3. Patch Operating Systems
4. Minimise users with Administrator access

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

RESPOND
Develop and implement the appropriate activities to manage cybersecurity risk to systems, assets, data, and capabilities.

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

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

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

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework
IDENTIFY Control Categories

Framework

<table>
<thead>
<tr>
<th>Function</th>
<th>Category Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY (ID)</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
</tbody>
</table>
# PROTECT Control Categories

<table>
<thead>
<tr>
<th>Function</th>
<th>Category Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTECT</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
</tbody>
</table>
**DETECT Control Categories**

<table>
<thead>
<tr>
<th>Framework</th>
<th>Function</th>
<th>Category Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td>DE.DP</td>
<td>Detection Processes</td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RESPOND Control Categories

Framework

<table>
<thead>
<tr>
<th>IDENTIFY</th>
<th>PROTECT</th>
<th>DETECT</th>
<th>RESPOND</th>
<th>RECOVER</th>
</tr>
</thead>
</table>

RESPOND (RS)

<table>
<thead>
<tr>
<th>Function</th>
<th>Category Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS.RP</td>
<td>Response Planning</td>
<td></td>
</tr>
<tr>
<td>RS.CO</td>
<td>Communications</td>
<td></td>
</tr>
<tr>
<td>RS.AN</td>
<td>Analysis</td>
<td></td>
</tr>
<tr>
<td>RS.MI</td>
<td>Mitigation</td>
<td></td>
</tr>
<tr>
<td>RS.IM</td>
<td>Improvements</td>
<td></td>
</tr>
</tbody>
</table>
RECOVER Control Categories

<table>
<thead>
<tr>
<th>Framework</th>
<th>Function</th>
<th>Category Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER (RC)</td>
<td></td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
• 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
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

It's QUESTION TIME!!
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
- Technology is ever evolving making us more and more connected - but this comes with ever evolving threats also
- Organisations need to up their levels of security controls to combat this

The Board  
Evolving Threats  
Uplift Security
Key Takeaways

The Basics

- Focus on the fundamentals first

People

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

Response

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

- Lots of Standards and Frameworks to measure your organisation against

- 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

- 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.