Connect › Support › Advance

The Institute of Internal Auditors Australia

Session 3A

Information security and privacy: A toolkit for government

Presented by

Michael Shatter
National Director, Security and Privacy Risk Services
RSM Australia

What are we covering today?

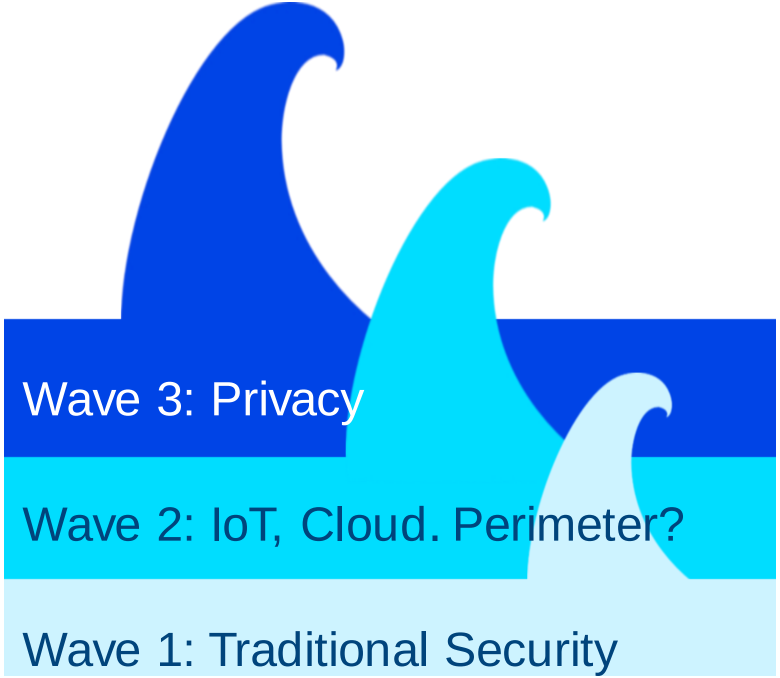
The Institute of Internal Auditors Australia

1. The Security Risk Landscape
2. Impact of Privacy
3. Security Fatigue
4. Human Capital Security Risks
5. Demonstrating Value

The Security Risk Landscape

- Attackers don’t differentiate between big and small targets
- Many systems are fully automated
- A breach can be dangerous if an attacker obtains password data that provides access to various systems.
- The end user is the easiest point in the network to attack
- Big breaches start with small compromises

The Security Risk Landscape

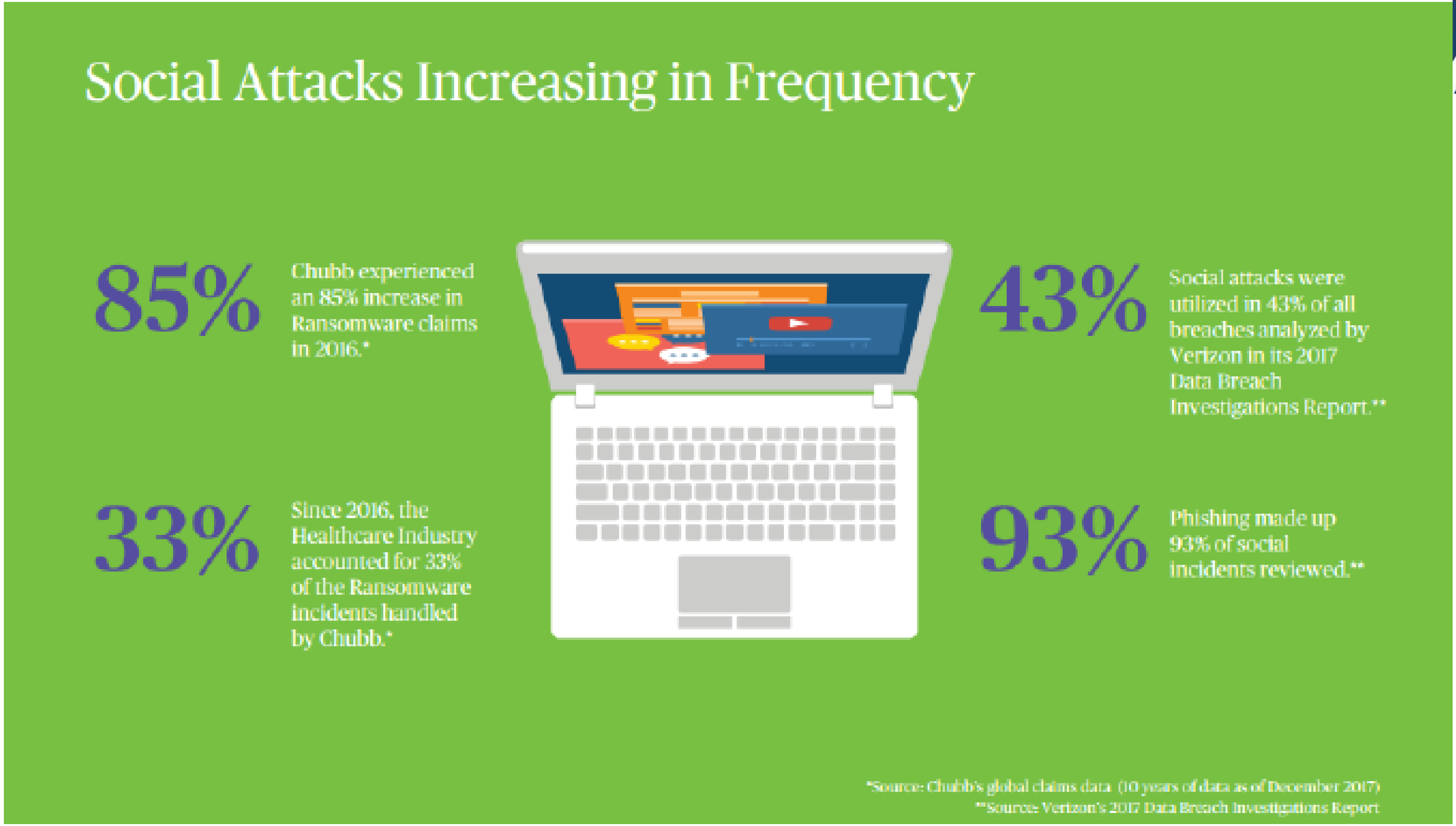


Wave 1: Defend company's data/crown jewels. Hundreds of devices.

Wave 2: Defend company's data/crown jewels. Explosive growth of attack surface (IoT, cloud, mobile). Thousands of devices.

Wave 3: Defend individuals' data. Millions of records – Erosion of Public Trust

Social Attacks Increasing in Frequency



Social Attacks Increasing in Frequency

85% Chubb experienced an 85% increase in Ransomware claims in 2016.*

33% Since 2016, the Healthcare Industry accounted for 33% of the Ransomware incidents handled by Chubb.*

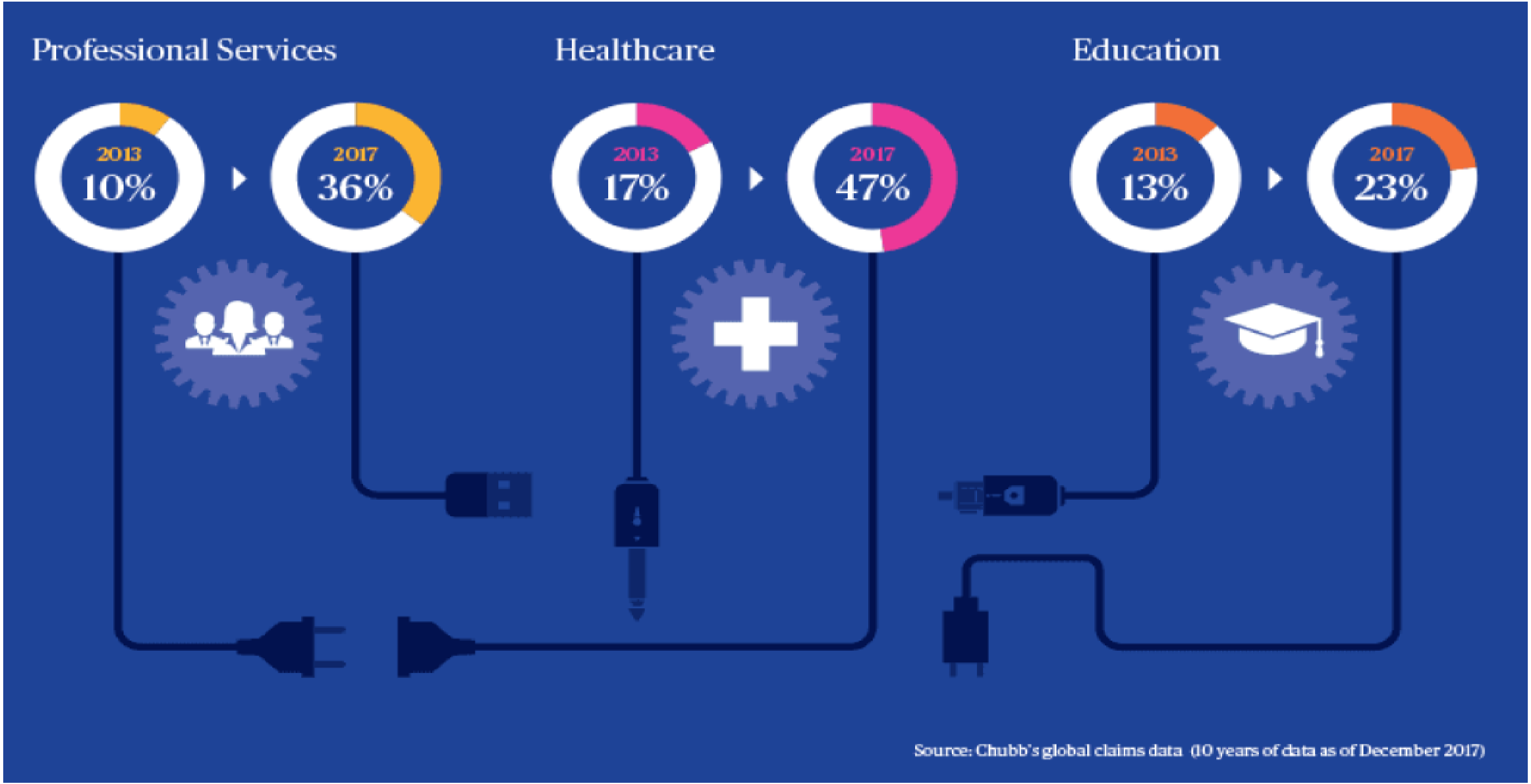
43% Social attacks were utilized in 43% of all breaches analyzed by Verizon in its 2017 Data Breach Investigations Report.**

93% Phishing made up 93% of social incidents reviewed.**

*Source: Chubb's global claims data (10 years of data as of December 2017)

**Source: Verizon's 2017 Data Breach Investigations Report

Incidents caused by human error are increasing in frequency



Source: Chubb's global claims data (10 years of data as of December 2017)

Privacy

- **Australian Privacy Principles – They do not apply to Councils…**

But…

- **National Data Breach Scheme applies**
  - Section 26WB – Recipients of TFN's
- **NSW Privacy and Personal Information Protection Act 1998 (PPIP Act) applies to local councils**
- **NSW Health Records and Information Privacy Act 2002 (HRIP Act) applies to local councils**

Security Fatigue

Human Capital Security Risks

Human Capital Security Risk

Human Capital Security Risks

- **Assess current security awareness**
  - Social engineering exercises
- **Develop a security awareness campaign**
- **Commit to the campaign across the organisation**
- **Update the campaign to reflect current risks**
- **Measure its effectiveness – Refine it or the approach**
- **Re-run it**

Demonstrating Value

The Institute of Internal Auditors Australia

- Public organisations have to justify budget investments
- Is the organisation paying too much for security?
- What’s the financial impact due to inadequate security
- When is security investment enough?
- Is the security product/service beneficial to the organisation?

Can be difficult to measure and report on the security investment

Demonstrating Value

Assessment & Analysis

- Should be treated in line with other business costs
- Reported on a periodic basis
- Communicated to stakeholders
- Comply with analysis process
- Include in decision making
- Refine
- Re-assess and Review

So to conclude

- **Test your security.**
- **Invest in but measure your security.**
- **Determine if you need a plan to address:**
  - Notifiable Data Breach scheme preparation
- **Know where your crown jewels are – Protect the castle.**
- **Have a breach response plan in place – Develop it, test it, update it and train on it**

Connect › Support › Advance

The Institute of Internal Auditors Australia

Thank you

QUESTIONS?