RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

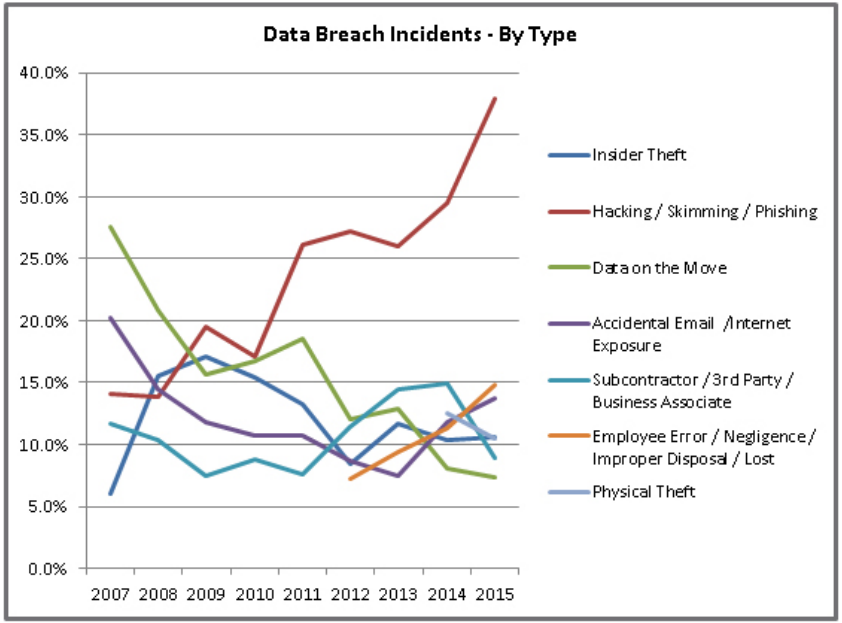
SESSION ID: CXO-W02

Real-world Examples of Positive Security ROI

John Pescatore
Director, Emerging Security Trends
SANS
@john_pescatore

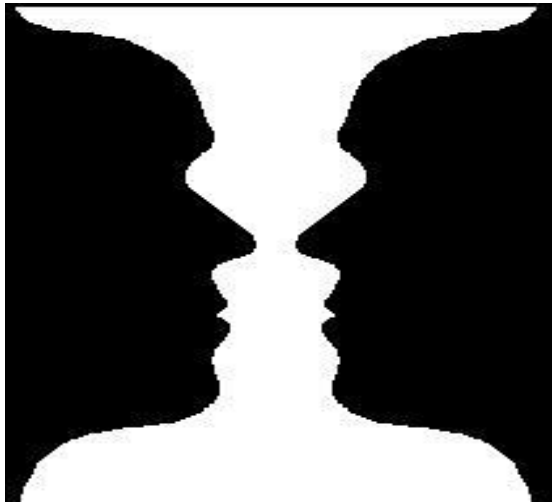
Some Perspective: 2015 Breach Statistics

- 781 breaches in 2015
  - What did the other 9,219 of the F10000 do differently?
- On average, 216K records exposed per breach
  - What did those who limited breach size do differently?
- 3,961 of 6,799 banks experienced physical crime in 2014

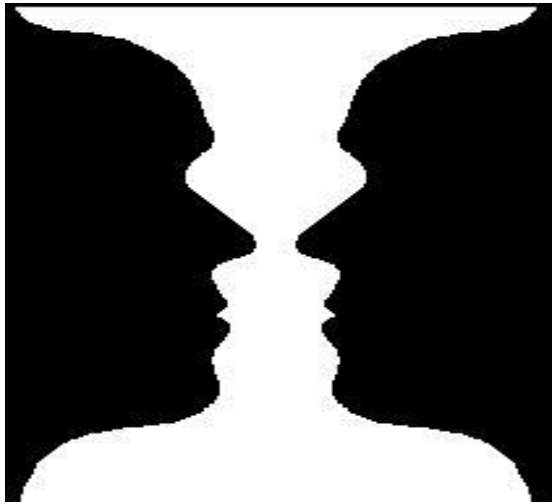


Source: Identity Theft Resource Center

Cybersecurity is Critical to Prevent Breaches



Cybersecurity is Critical to Enable Business

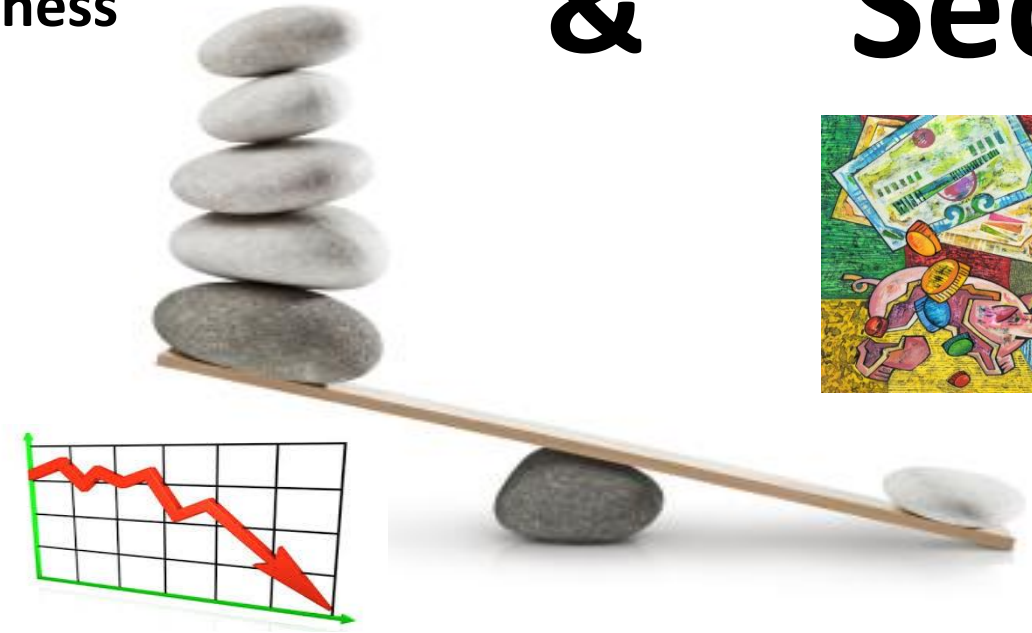


Balancing Business & Security

Balancing

Business & Security

Balancing Business & Security



Opening Stipulations

- It's Dangerous Out There, Fine
- Security Is Hard, Will Continue to Be Hard
- Business Goes On, With or Without Security
- **CEOs and Boards understand safety and they understand protecting people – customers and employees**

Security is Already At the Business Table

Business View of Cybersecurity Math

Risk = Threat x **Vulnerability** + Action

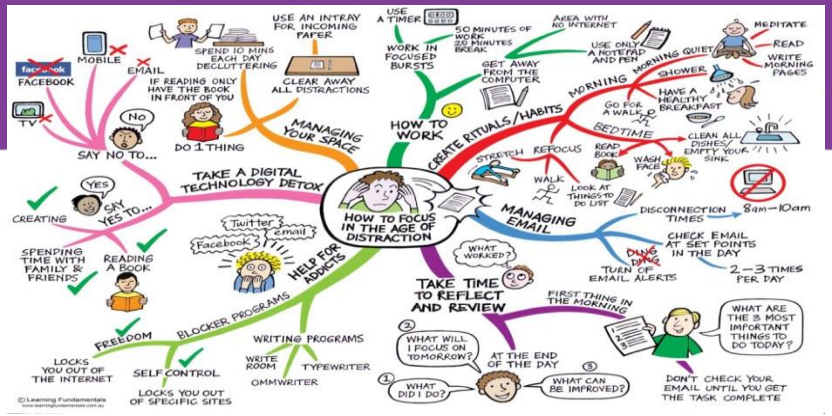
Potential Impact = Risk X **Cost**

Financial Impact = Potential Impact – Insurance Payoff

Cost = %Successful attacks X (Downtime/Breach costs +Response/Cleanup) + Cyber Defense "Friction"

- The goal is reduce the impact to the bottom line:
  - Reduce vulnerabilities
  - Prevent more attacks
  - React faster/more surgically to incidents
  - Restore more quickly
- **"Security buys a lot of products – where is the connection to a safer business?"**

SANS



Focus on protecting the business first

Effectively **and** efficiently **and** quickly

Make sure the solution isn't worse than the problem

Compliance must **follow** security

Is it Safe Enough for Us to Self-insure?

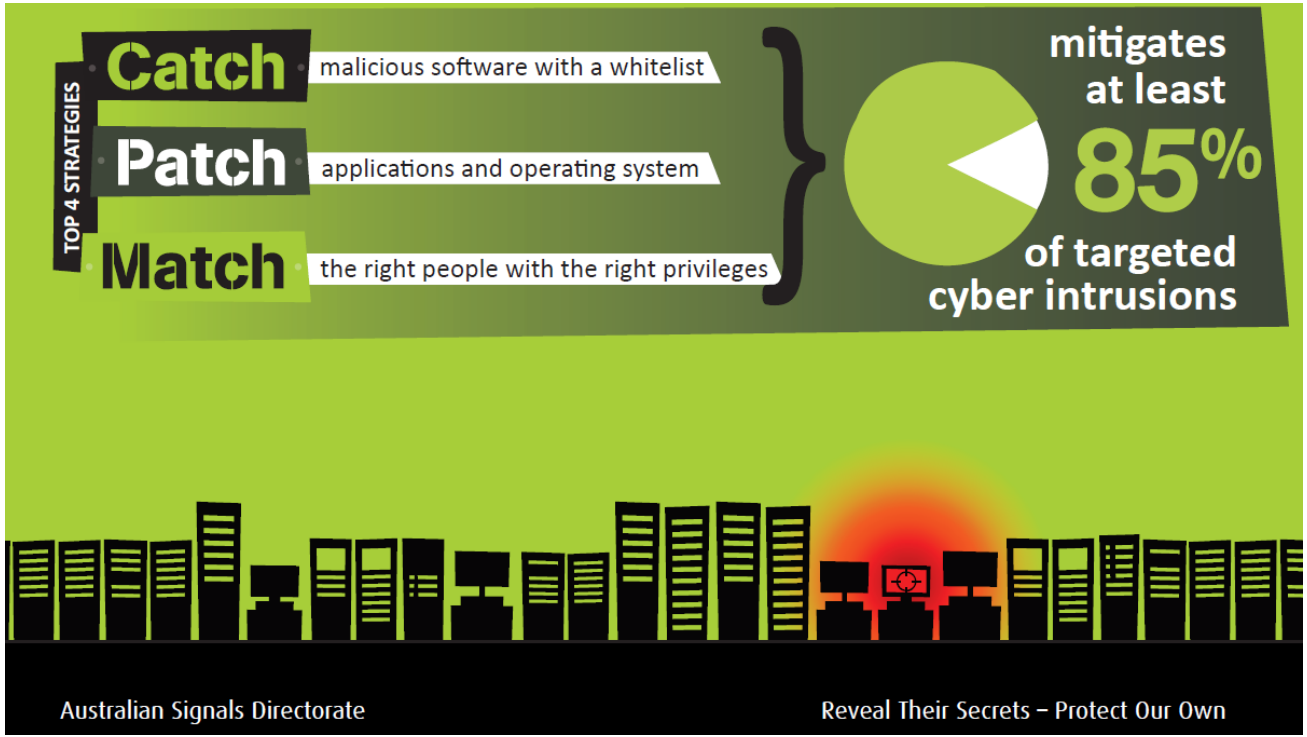
SANS WHAT WORKS In Internet Security

Summary of Last Year's Examples

- **Higher Ed** - Intrusion Detection Rate **increased** 46%, corrective actions costs **decreased** 35%
- **Financial Sector**– reduced PC reimaging due to malware from **4 per week** to **1 every 3 months**, and will enable the use free of AV on desktops
- **Software** – use of managed bug bounty approach increased critical vulnerability discovery 10x for same cost, decreased fix time.
- **Healthcare** – maturity in secure app dev life cycle **reduced time to market for new app by 30% and reduced software development costs by 15%**

SANS

Update: Australian ASD Top 4



Meeting Demands for Collaboration

- Problem: Electronic trading environment includes 40,000 firewall rules with 5,000 added annually. Two FW admins could not keep up with change requests, high error rate.
- Solution: Enhance firewall policy management process
- Results:
  - **Reduced** FW rule change assess to approve from 1 person-month to 1 person-day.
  - **Reduced** error rate and **reduced** time demonstrating compliance to auditors

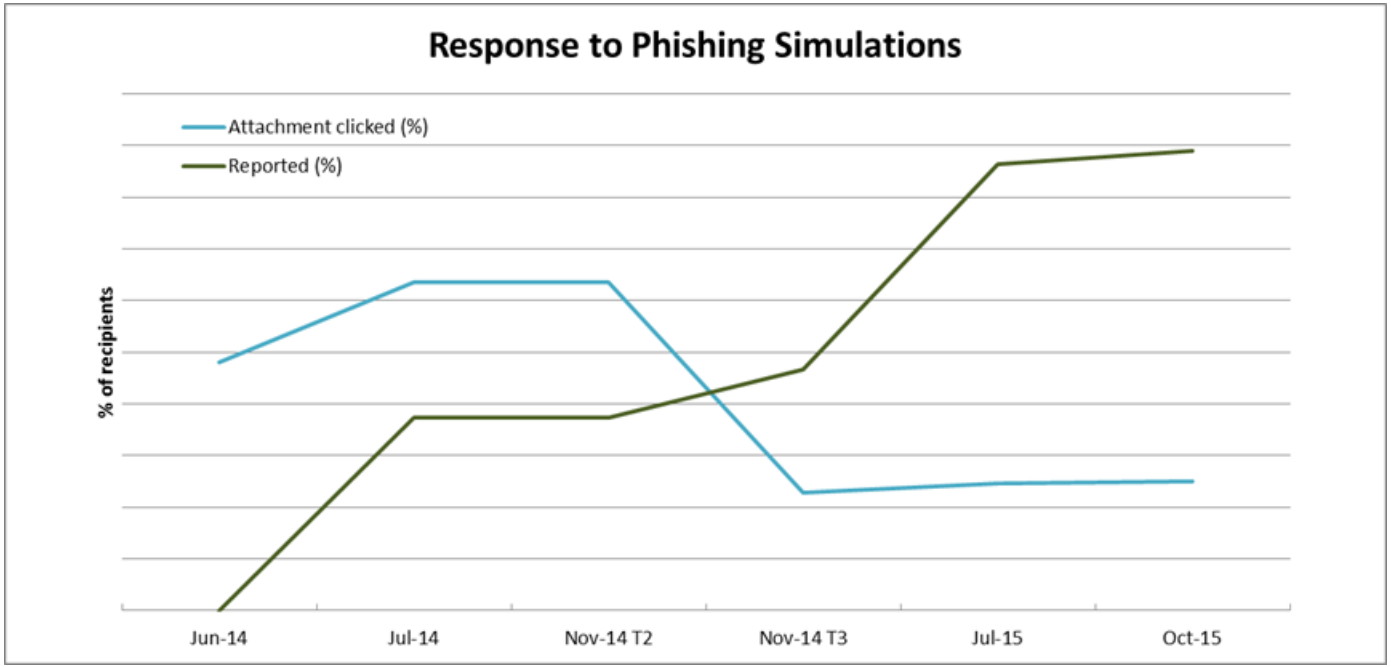
SOC Staff Overload

- Problem: Even with constant tuning of IDS system, time to discover actual incidents resulted in excessive business impact.
- Solution: Evaluate and update IDS architecture
- Results:
  - Daily alert rate **reduced** by 99%
  - False positive rate **decreased** 99.8%
  - No change in false negative rate.

Reducing Phishing Impact

- Problem: Mid-sized European financial services company continued to see phishing-initiated incidents increase despite a security awareness program.
- Solution: Use phishing simulation/testing to first demonstrate seriousness. From there engage with C-level management for support to drive behavior change and needed controls. Obtain funding for continued multi-channel effort to reduce “click on bad stuff” rate.

Results


Response to Phishing Simulations
Attachment clicked (%)
Reported (%)
% of recipients
Jun-14
Jul-14
Nov-14 T2
Nov-14 T3
Jul-15
Oct-15

Speeding Up Third Party Certification

- Problem: Large financial institution has over 1,500 vendors and business partners. Third party due diligence team takes too long to add new vendors and has no ability to do continuous monitoring.
- Solution: Similar to lending operations, use a credit score approach
- Result: Existing staff can now track 3rd party risk on a weekly basis. Able to quick start new vendors while detailed vetting in process. Extend visibility out to Business Unit management.

A Few Others

- **DNS Sinkholing** – essentially free added layer of phishing/drive-by protection
- **Load balancer/CDN filtering** – web application firewalling without having to buy/administer another product.
- **SOC Tools, Services** – skills first, but hunting automation, "playbook as a service" offerings out there as staff augmentation/force multipliers.

When You Get Back to Work

- Make sure you are collecting the right security metrics so you can demonstrate value, improvement, danger.
- Any major transitions coming:
  - Moving to Windows 10, cloud services, mobile apps, agile dev, etc.
  - M&A, re-org, new C-level management.
  - Audit results
- Prioritize by business impact – shoot for a near term win.

Resources

- SANS What Works - http://www.sans.org/critical-security-controls/case-studies
- Critical Security Controls - http://www.counciloncybersecurity.org/critical-controls/
- PCI Prioritization Guidelines - https://www.pcisecuritystandards.org/security_standards/prioritized.php
- NSA Top Ten - https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_Top10IAMitigationStrategies_Web.pdf