The Cyber Landscape and Your Culture of Security

MASBO Conference
May 12, 2017

Introduction

Jon Ault
Technology Consulting | Cyber Security Leader
• 20+ years in Technology Consulting
• 7 years of Education technology experience
• Passion for designing client centric security solutions

Agenda

• Cyber Security Landscape
• Challenge of Cyber Security
• Management’s Greatest IT Needs – Where to Start
• Establishing a Culture of Security
“The severity and impact of cyberthreats have changed the landscape in which governments, corporations, individuals and, specifically, financial institutions of all sizes and complexities operate.”

Department of Defense | Cyber Strategy

**Top Risks for the United States per DoD**
1. Cyber Threats
2. Terrorism
3. Transnational Organized Crime

---

**Risk is Everywhere**

---

**All Data Has Value**

Per Identify Theft Resource Center (2005-2015 data)

- Total of 5,810 reported data breaches
- Estimated loss $47,897,830 known compromised records
- Out of 1,600 security sensors | 96% detected breach traffic

---

**Shocking Truth**

99.9% of breaches could have been prevented …

Identity Theft Resource Center 2005-2015
## What's your Data Worth?

**Advertised Prices on the Black Market**
- US based credit card with verification | $1-$6
- An identity (including US Bank Account, credit card, date of birth, and gov. issued ID) | $14-$18
- List of 29,000 emails | $5
- Online bank account with $9,900 balance | $300
- Phishing Website Hosting | $3-$5
- Verified PayPal Account with balance | $50-$500
- Skype Account | $12
- One month World of Warcraft Account | $10

### Value to a Hacker

- 40M records sold for $2 per / $80M in profit

---

## K-12 Security Breaches

You don't have to look far to find K-12 relevant breach data . . .

---

### K-12 Security Breaches

Threats of all types . . .
- Phishing Attack
- Accidental Disclosure
- Ransomware
- Denial of Service

---

---
**Dam Hackers**

March 25, 2016 Headline: 7 Iranians charged with hacking attacks on US Banks and a dam in New York

**How to Hack a Dam**

Used Google Dorking
- Identifies unprotected computers
- Technique has been around for 10 years and is neither illegal nor always malicious

Computers often predate the internet and are not protected

Per US Attorney of New York – it’s a “frightening new frontier…”

**Yahoo Security Breach**

What we know

Yahoo internal investigation found indications that a state-sponsored actor had stolen data in 2014.

Hackers stole personal information for over 500 million accounts
- names
- email addresses
- phone numbers
- birthdates
- security questions and answers
- “hashed” passwords

![Yahoo Hack Logo](image)
Exploiting Yahoo Data

Users often use the same password on multiple accounts

The Challenge of Cyber Security

Prince William at Royal Air Force Base

The Challenge of Cyber Security

Prince William at Royal Air Force Base
**Target Security Breach**

Spring 2013 – Target installs FireEye network monitoring software
Sept 2013 – Target certified as meeting PCI standards

Nov 30 – Hackers deployed custom-made malware (detected by FireEye)
Dec 2 – Hackers begin moving credit card data out of Target’s network (detected by FireEye)
Dec 12 – Target notified of data breach by Federal investigators.
Dec 15 – Target confirmed malware was removed.

**Impact of Target Breach**

Tangible Costs
- $148M | Breach
- $100M | Better Security
- $86M | VISA & MasterCard Settlement

And then some...
- CEO | FIRED
- Board of Directors | SUSTAINED CLASS ACTION LITIGATION FOR NEGLIGENCE
- Customers | UNKNOWN NUMBER LOST

**Our Greatest Need**

Boards and Executives need two things from IT

TRANSPARENCY | INDEPENDENCE
In general, IT Departments operate in one of three communication models.

1. Proactive
2. Willing *Most Organizations*
3. Hostile

**Challenge for Management**
Which questions to ask IT?

---

**Independence**

The most likely architects of cyberattacks are system administrators or other IT staff with privileged system access.

*U.S. Computer Emergency Readiness Team (CERT)*

---

**Why Treat IT Any Differently?**

Look to Finance and Accounting industries as guide
- Experts provide transparency
- Evaluation is independent of the entity
Establishing a Culture of Security

Set the Tone from the Top

Identify, measure, mitigate and monitor risks

Develop risk management processes

Align IT strategy with business strategy

Create a governance process

Report meaningful & timely metrics

www.eidebailly.com/cybersecurity

Your Culture of Security

Prevention

- Establish budgets
- Follow best practices
- Obtain advance training
- Employ appropriate expertise
- Operationalize security into everyday duties of everyone
- Strategize to prevent every ATTEMPT

www.eidebailly.com/cybersecurity
Your Culture of Security

Detection
- Establish centralized logging / reporting
- Collect logs from all systems, networks, applications and all reported issues
- Correlate and aggregate all logs
- Setup rules and signature databases for alarms and alerts
- Collection should have no filters – no hack is too small
- Establish robust search, filtering and reporting capability
- Strategize to detect every ATTEMPT

Your Culture of Security

Response
- Establish a response capability / team
- Review reports from monitoring activities
- Meet regularly to make informed decisions / updates / budgets
- Strategize to respond to EVERY ISSUE
- "Making an informed decision to do nothing is acceptable but beware of the consequences... (don't be immune)"

Your Culture of Security

Remember
- Each of you can have a significant impact on security culture within your organization.
- Security is NOT a one-size-fits-all proposition.
- Build a security strategy
- Build a monitoring plan into your ongoing process.
- This process never sleeps!