The Cyber Landscape and your Culture of Security

HFMA – Region 9 Webinar
November 15, 2016
Introduction

Jon Ault
Eide Baily Technology Consulting | Cyber Security Leader

- 20+ years in Technology Consulting
- Passion for designing client-centric security solutions
- 10+ years of health care industry experience

www.eidebaily.com/cybersecurity
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 cyber threats have changed the landscape in which governments, corporations, individuals . . .

Risk is Everywhere

“The severity and impact of cyber threats have changed the landscape in which governments, corporations, individuals . . .”

Department of Defense | Cyber Strategy

Top Risks for the United States per DoD
1. Cyber Threats
2. Terrorism
3. Transnational Organized Crime
All Data Has Value

Per Identify Theft Resource Center (2005-2015 data)

• Total of **5,810 reported** data breaches

• Estimated loss **847,807,830 known compromised records**

• Out of **1,600 security sensors** | **96%** detected breach traffic

• Mid-way through 2016 there have been **142 HIPAA breaches** involving 500+ patient records (Source: HIPAA Journal)
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
- One Personal Health Record | “Up to hundreds”
- 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

www.eidebailly.com/cybersecurity
High Profile Incidents – Outside of Health Care

Even some non-health care breaches have the potential to impact your organizations . . .

• Yahoo Case Study
  • Passwords

• Target Case Study
  • Credit Card Information

• Our “cyber lives” are unavoidably linked!
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
• birthdays
• security questions and answers
• “hashed” passwords

www.eidebailly.com/cybersecurity
Exploiting Yahoo Data

Users often use the same password on multiple accounts

Security questions and answers

Use to reset password

Password (hashed)

Decrypt if easily guessable

www.eidebailly.com/cybersecurity
**Target Security Breach**

**Spring 2013** – Target installs FireEye network monitoring software.

**Sept 2013** – Target certified as meeting PCI standards.

**Dec 12** – Target notified of data breach by Federal investigators.

**Dec 15** – Target confirmed malware was removed.

**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).

![Map of Target Monitoring Locations](www.eidebailly.com/cybersecurity)
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

www.eidebailly.com/cybersecurity
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?
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
Establishing a Culture of Security

- Identify, measure, mitigate and monitor risks
- Report meaningful & timely metrics
- Develop risk management processes
- Set the Tone from the Top
- Create a governance process
- Align IT strategy with business strategy
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
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)"

www.eidebailly.com/cybersecurity
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!

www.eidebailly.com/cybersecurity
Jon Ault
Cyber Security Leader

701.205.9940
jault@eidebailly.com

#EIDELIKE
I'd like to understand where to start with Cyber Security

EideBailly

www.eidebailly.com/cybersecurity