Center for Internet Security®

IBANYS 2018

Ryan Spelman
Senior Director, Business Development

The Center For Internet Security

The Test At The End Is Worth 35% Of Your Final Grade

The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization focused on enhancing the cybersecurity readiness and response of public and private sector entities.

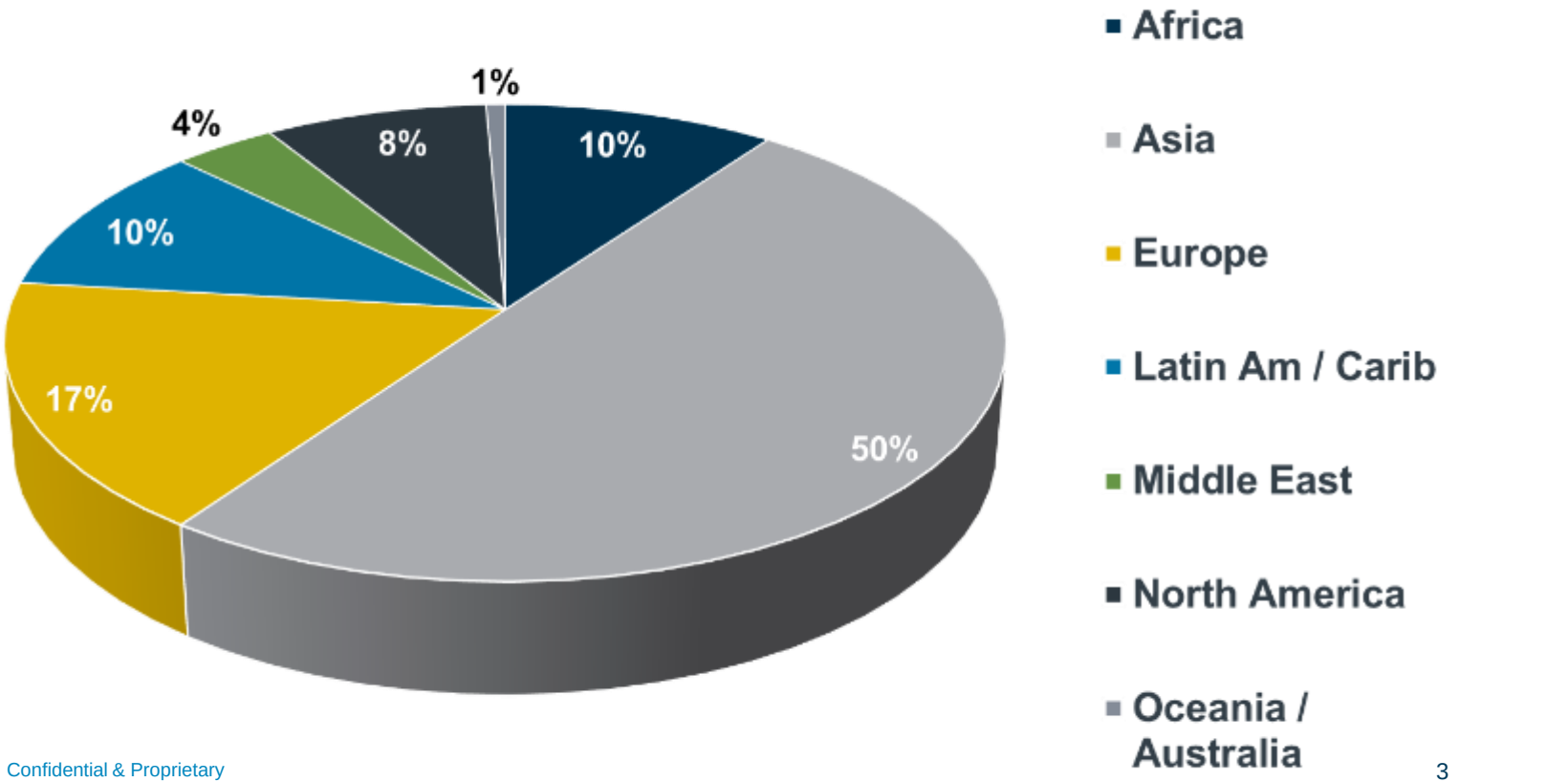
Organizations have to defend the rapidly increasing digital infrastructure while at the same time complying with ever changing information security regulations.

We will discuss evolving threat trends and the best practice solutions designed to combat them.

Hard questions welcomed! Easy questions encouraged!

Everybody Is On The Internet!

Is That A Good Thing… Discuss!



What Is The Risk?

I Grade On A Curve

Risk =Threat x Vulnerability x Cost

Internet of Things

Why Are You Hacking My Data, Kit?

Hacking worries grow for Web-connected cars

As the Chrysler recall shows, the auto industry is coming to grips with dangers of connecting cars to the wider world.

By AARON M. KESSLER New York Times | JULY 28, 2015 — 6:52PM

IoT DDOS

A New Spin On An Old Favorite

- Mirai Botnet Attack
- Hacking of DVRs, security cameras, and other devices took down major internet services provider
- Actor unknown

Financial Breakdown

Time Is Money!

- The Average Data Breach Cost $4 Million
- Each Record Cost $158
- 50 days average time to resolve a malicious insiders attack
- 23 days average time to resolve a ransomware attack

Insurance Industry is Catching up to Technology

The Wild West of Insurance

- 102% Growth in Premiums from 2012 to 2016
- Cyber Insurance is projected to go from $2 Billion in premiums today to $20 Billion by 2025

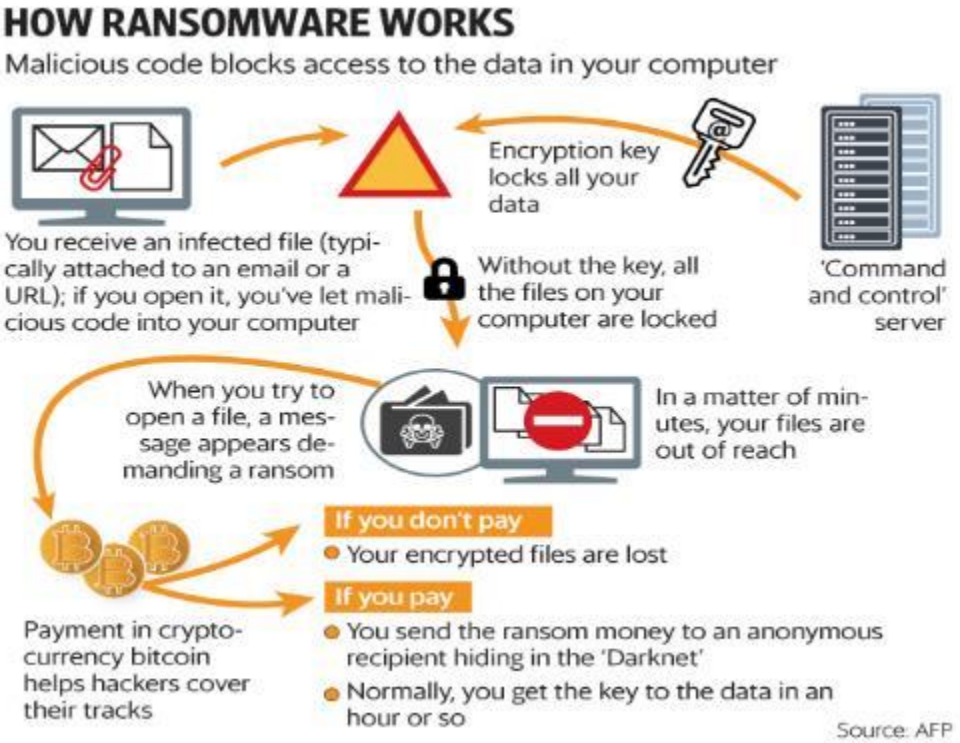
Attacks

There Are More Types, These Are My Favorites

- Ransomware
- Lost/Stolen Device/Data
- Phishing

Attack: Ransomware

I Am Sure You Have Heard About This



Attack: Ransomware (continued)

I'd Dispute The Ransom Fee Being Added To The Bill…

Luxury Hotel Goes Analog to Fight Ransomware Attacks

Written by
DANIEL OBERHAUS
CONTRIBUTOR

29 January 2017 // 01:26 PM EST

Attack: Lost/Stolen Laptop

Who. Does. This.

- 3,576 Laptops
- 3,444 tablets or smartphones
- 996 USB devices…

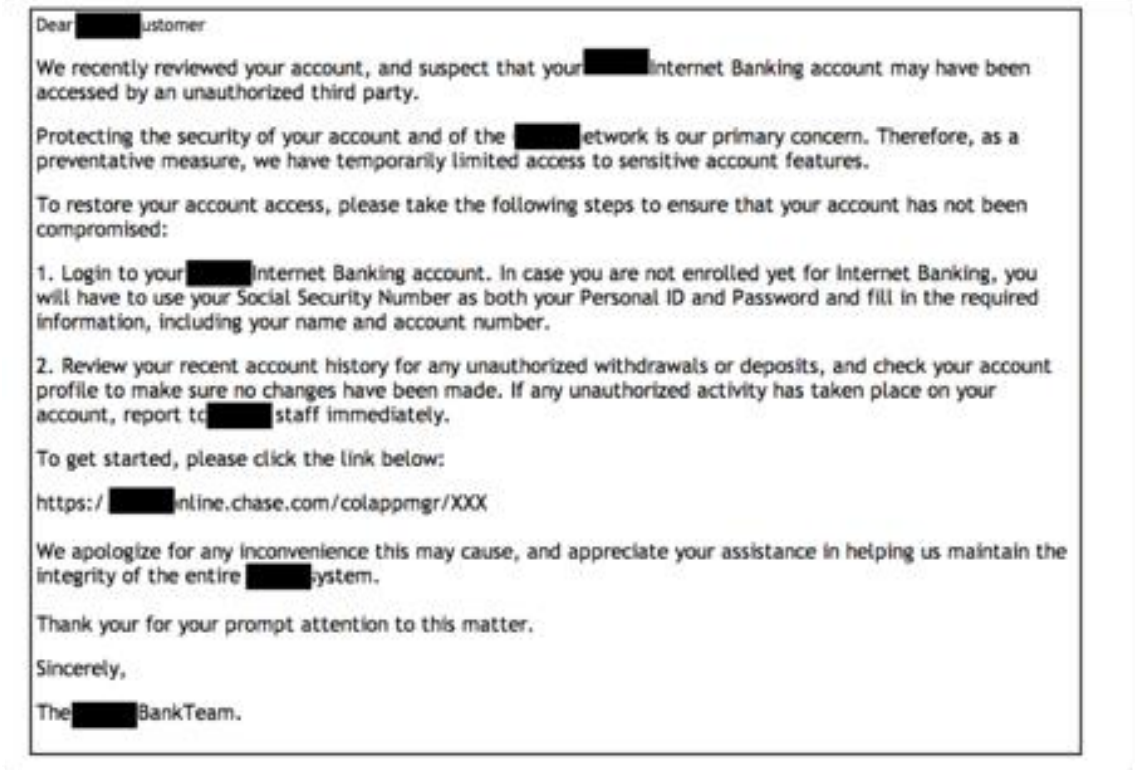
Were left at airports from June 2011 to June 2012

About half were eventually recovered.

The rest were turned over to authorities or donated to charity

Attacks: Phishing

It's A Trap!



Dear [redacted]ustomer

We recently reviewed your account, and suspect that your [redacted]internet Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account and of the [redacted]etwork is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your account access, please take the following steps to ensure that your account has not been compromised:

1. Login to your [redacted]internet Banking account. In case you are not enrolled yet for Internet Banking, you will have to use your Social Security Number as both your Personal ID and Password and fill in the required information, including your name and account number.

2. Review your recent account history for any unauthorized withdrawals or deposits, and check your account profile to make sure no changes have been made. If any unauthorized activity has taken place on your account, report t[redacted]staff immediately.

To get started, please click the link below:

https:/ [redacted]nline.chase.com/colappmgr/XXX

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire [redacted]ystem.

Thank your for your prompt attention to this matter.

Sincerely,

The [redacted]BankTeam.

Compliance

Does Anyone Know What These Acronyms Mean?

- Loss of community/customer trust
- NYS DFS
- SEC
  - Yahoo was just fined $35 Million for not reporting breach
- GDPR

Montana

Wait A Second, That Is More Than The Total Population!

- 1.3 Million People Notified
- Full Forensic Analysis Done
- $2 Million dollar insurance policy utilized for direct costs (such as mailing)
- To date, no one has notified them that their information was used!

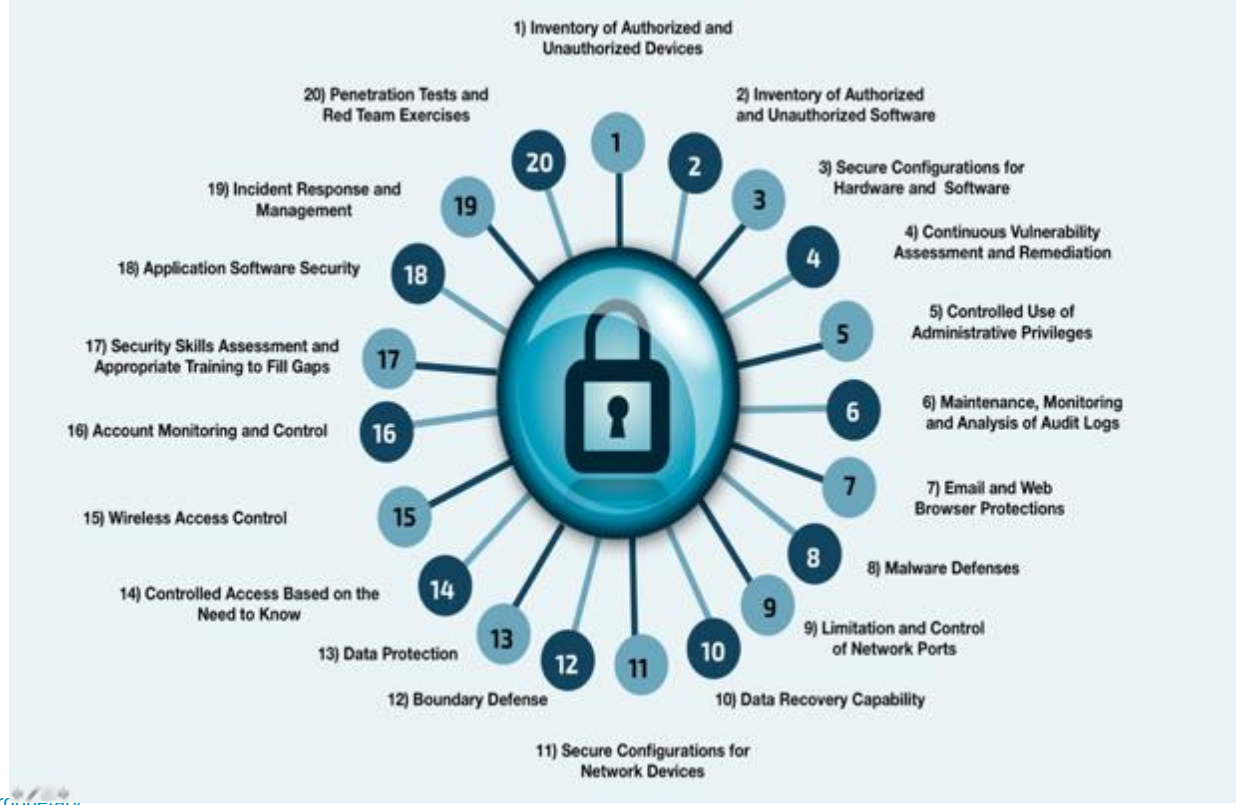
Wendy's

Data Breach On The Side Please!

- Wendy's had a breach of its payment processing system
- Potentially millions impacted
- Third party compromise suspected
- Lawsuits still pending – Costs could be higher then Target Breach

CIS Critical Security Controls

Previously Doing Business As The SANS Top Twenty



Count

You Can’t Protect What You Don’t Know About!

- Do you have the means of identifying unauthorized devices?
- Risk: Devices and software added to your network without your knowledge can be accessed by malicious actors without your permission
- Make a list of all assets
- This list should include all hardware and software, including devices such as printers and scanners

Patching

I Think I Did A Joke On This Already…

- Do you apply security patches to operating systems and applications on a regular basis?
- Why is this critical:
  - Unpatched systems are one of the primary ways attackers gain access. A good patching practice reduces the risk of exploitation.
- What does it look like?
  - You patch operating systems and applications on a regular basis.

Control

Calling Maxwell Smart!

- Do you limit the number of users with administrative privileges?
- Why is this critical:
  - Administrative privileges are keys to the kingdom.
  - If an admin gets “infected” it’s a **big** problem.
- What does it look like?
  - No end users with administrative privileges.
  - Ideally, limit privileges to just the Network and/or System Administrators (and it is validated!).

Configure

Travelling Is Killing My “Configuring”

- What are industry-accepted configurations/standards?
  - Includes NIST, CIS Benchmarks, and others
  - Covers items like password length, encryption, and port access
- Why is this critical:
  - Most software and hardware out of the box is only partially securely configured. You aren’t born fit… you have to work at it!
- What does it look like?
  - You have a standardized hardened image.
  - Follow strict configuration management (change control board)

Why Is This Hard?

Eat Your Vegetables, Said Every Parent Everywhere

We need all configuration changes reviewed by the change control board and signed off by a senior exec

We can make any change our users need to configurations, especially if its really important for them to fulfill their business objective

Maintenance, Monitoring and Analysis of Audit Logs

If You Have 1,000 Attempts A Second…

- Do you continuously monitor your logs (firewall, system and web logs) for anomalies and security violations?

- Why is this critical:
  - Failure to monitor logs increases the risk that a pattern of behavior that may indicate a data breach will go undetected.

- What does it look like?
  - You are logging activity and monitoring the logs for the appropriate amount of time.

Email and Web Browser Protections: Black/White Listing

Black Magic And White Magic Sounds Cooler

- Do you employ email attachment white listing/black listing practices?
- What is white listing/black listing?
  - White listing: the practice of only allowing specific file types into your email
  - Black listing: the practice of denying specific file types into your email
- Why is this critical:
  - Email attachments are one of the primary methods by which attackers seek access to the network. Both black listing and white listing can limit your exposure to this risk.
- What does it look like?
  - You are utilizing either black listing or white listing (white listing is preferred, although it is harder).

Malware Defenses: Firewalls, Anti-Malware, and IPS

No Alerts For 3 Months Is A Problem

- Employ automated tools to monitor workstations, servers, and mobile devices with anti-malware, personal firewalls and host-based IPS functions
- Why is this critical:
  - Anti-virus “quarantines” malicious programs and minimizes the risk that they may do damage
  - Failure to update anti-virus reduces its effectiveness
- What does it look like?
  - Tools are in place, updating, and reporting to a centralized platform AND it is updating

Limitation and Control of Network Ports

Who Doesn’t Love Surprises!

- Do you manage the ongoing use of ports, protocols, and services on networked devices in order to minimize vulnerabilities.

- Examples:
  - Web servers
  - Mail servers
  - File or print servers

Double check what you install (vendors sneak in extras)!

Data Recovery Capability

Keep Some Back-ups On A Separate Network… Pretty Please?

- Do you have a process to properly back up critical information with a proven methodology for timely data recovery.

- Why is this critical:
  - Key in response.
  - Criminals have been known to subtly modify data.

- What does it look like?
  - You are backing up data frequently and periodically, including operating system and application data.
  - Backups are tested!

Additional Resources

Engage CIS!

Questions?

Ryan.spelman@cisecurity.org