

Lutz

MIND WHAT MATTERS

CYBERSECURITY SIMPLIFIED

PRESENTED BY: SCOTT KROEGER

AGENDA

- **CYBER SECURITY SIMPLIFIED**
 - Framework for thinking about security in your organization
- **IF YOU ARE BREACHED....**
- **HOW TO PROTECT YOUR BUSINESS**
- **HOW TO PROTECT YOU AND YOUR FAMILY**
- **Q&A**

CYBER SECURITY - HEADLINE NEWS

CYBER SECURITY

A New Headline
Every Day

U.S. to establish new cybersecurity agency

BY WARREN STROBEL

WASHINGTON | Tue Feb 10, 2015 10:12am EST

Anthem Hacking Points to Security Vulnerability of Health Care Industry

By REED ABELSON and MATTHEW GOLDSTEIN

CEO heads may roll for security breaches in wake of Sony boss' exit, experts say

Feb 9, 2015, 6:54am PST

Brokerage Firms Worry About Breaches by Hackers, Not Terrorists

By MATTHEW GOLDSTEIN FEBRUARY 3, 2015 11:54 AM 4 Comments

Sony PlayStation and Microsoft Xbox Live Networks Attacked by Hackers

By NICOLE PERLROTH and BRIAN X. CHEN DECEMBER 26, 2014 4:11 PM 31 Comments

F.B.I. Says Little Doubt North Korea Hit Sony

By MICHAEL S. SCHMIDT, NICOLE PERLROTH and MATTHEW GOLDSTEIN JAN. 7, 2015

HEADLINE NEWS – AUGUST 2016

- The U.S. Department of Health and Human Services Office of Civil Rights (OCR) made headlines this month with a record \$5.55 million HIPAA settlement reached with Advocate Health Care System, Illinois' largest health care system
- 3 different data breaches
- 4 million individual patient records

'SMALLER SIZED' BREACH INITIATIVE

- Hospice of Northern Idaho – \$50,000 settlement in 2013 as a result of 2010 theft of unencrypted laptop computer from an employee's car, with electronic PHI (ePHI) of 441 individuals.
- QCA Health Plan of Arkansas – \$250,000 settlement in 2014 following a 2012 theft of unencrypted laptop computer from an employee's car, with ePHI of 148 individuals.

'SMALLER SIZED' BREACH INITIATIVE

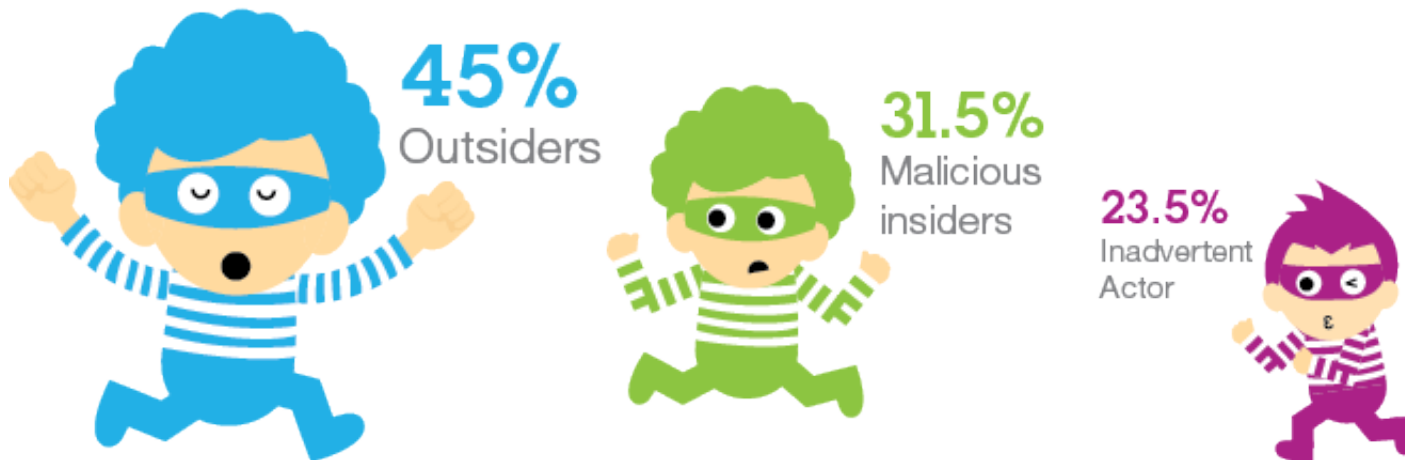
- St. Elizabeth's Medical Center – \$218,400 settlement in 2015. Massachusetts hospital's 2012 report of workforce members using an Internet-based document sharing application to store ePHI of at least 498 individuals plus 2014 breach of ePHI on a former workforce member's personal laptop and USB flash-drive.
- Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) – \$650,000 settlement in July 2016 after theft of unencrypted iPhone of employee, with ePHI from 412 residents of six nursing homes for which CHCS was providing management and information technology services.

CYBER SECURITY SIMPLIFIED

- **TWO TYPES OF THREATS**

- Internal (55%)
- External (45%)

Who are the “bad guys”?



MALICIOUS INSIDERS

- **INSIDER THREAT**

- Insider threats exist within every organization
- Why? - As a result of some perceived injustice, retaliation, a sense of entitlement, an unwitting need for attention and/or validation, the employee takes some action as part of a contrived solution that results in negative consequences for an organization
- Typically a result of excessive internal privilege



MALICIOUS INSIDERS

INSIDER



DISGRUNTLED EMPLOYEE

- Terminated
- Disagreement with management
- Disagrees with policy change



INSIDER WITH ACCESS

- Insider with elevated privileges



TYPES OF LOSS

- Patient data / HIPAA data
- Proprietary Practice Information
- Private Physician Information
- Financial Account Manipulation
- Media Leaks



INTERNAL THREAT – INADVERTENT ACTOR

UNWITTING SUSPECTS







- Passwords
 - *Easy to guess*
 - *Never change*
 - *Same Password*
- Clicks links in emails
- Poor surfing practices
- Leaves mobile devices/laptops unattended and unlocked
- Installs software that contains virus / malware
- Uses open WiFi

23.5%

Inadvertent
Actor



OUTSIDERS / EXTERNAL THREATS

THREATS	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
						
MOTIVATION	Hactivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

EVOLUTION OF CYBERCRIME

OLD

Hacker Organization

- Centralized
- Build from scratch
- Own servers
- Expensive
- Large targets

CRIME



NEW

Crime Ecosystem

- Distributed
- Buy or hosted
- Specialize in areas
- Cheap
- Smaller targets

CYBERCRIME IS EASIER THAN EVER

AND IT'S MORE ACCESSIBLE TO EVERYONE

Постоянно требуется написание
автозаливных инжектов под

Zeus/SpyEye

от **2000\$** за
выполненный
проект

JOB POSTINGS



WebMoney



Perfect Money
Just perfect

PAYMENT SYSTEMS



**Silk
Road**

anonymous marketplace



Hydra

MARKETPLACES

CYBERCRIME COSTS

CRIME



BUSINESS EMAIL COMPROMISE:

Targets are typically C-Level Executives

October 2013 to August 2015:

- Total U.S. Victims: 7,066
- Total U.S. exposed dollar loss:
\$747,659,840.63

EXTERNAL THREATS

- Viruses (Malware, Spyware, Viruses, Worms, Trojans, Bots)
- Virus Aftereffects (Backdoors, Exploits)
- Unknown Software Vulnerabilities
- Hackers
- Phishing (Fake Electronic Email)
- Social Engineering

VIRUSES

CRIME



- Cryptolocker / Cryptowall



MALWARE

CRIME



HOW DO YOU GET MALWARE?

- Internet ads
- Malicious emails
- Hacked websites



PHISHING (FAKE EMAIL)

SPEAR PHISHING

- Email contains attachment or link which recipient is likely to open
- Crafted to appear to come from a trusted source
- Attachments tailored to recipients likely interest
- Broad address and personnel information are available open source.



EMAIL SCAMS

CRIME



From: Mike [REDACTED] Sent: Mon [REDACTED]
To: [REDACTED]
Cc: [REDACTED]
Subject: Fw: Wiring Instructions

Message [REDACTED] LLC WIRING INSTRUCTIONS.pdf (27 KB)

Process a wire of \$73,610 to the attached information, and code it to professional expenses. I will forward support later. I have cc'd the beneficiary, email them the transfer confirmation when you have it.

----- Original Message -----
Sent: Monday, February 23, 2015 at 9:54 AM
From: "Jen"
To: "Mike"
Subject: Wiring Instructions

Per our conversation, I have attached instructions for the wire. Let me know when it has been processed.

PHISHING EXAMPLES

phughes@unicogroup.co
phughes@unicogruop.com
phughes@unicogroup.com
PHUGHES@UNICOGROUP.COM

**INTENTIONALLY SMALL AS IF YOU WERE
LOOKING AT YOUR PHONE OR ADDRESS
LINE ON A COMPUTER**

PHISHING EXAMPLES

phughes@unicogroup.co

phughes@unicogruop.com (o/u transposed)

phughes@unicogroup.com

PHUGHES@UNICOGROUP.COM ('L' not 'I')

Yes! Your domain is available. Buy it before someone else does.

unicogruop.com

☐

unicogruop.us Add this: \$1.00

when you register for 2 years or more. 1st year price \$1.00 Additional years \$19.99

~~\$14.99*~~ **\$2.99***

when you register for 2 years or more.
1st year price \$2.99 Additional years \$14.99

Select

unlcogroup.com

☐

unlcogroup.us Add this: \$1.00

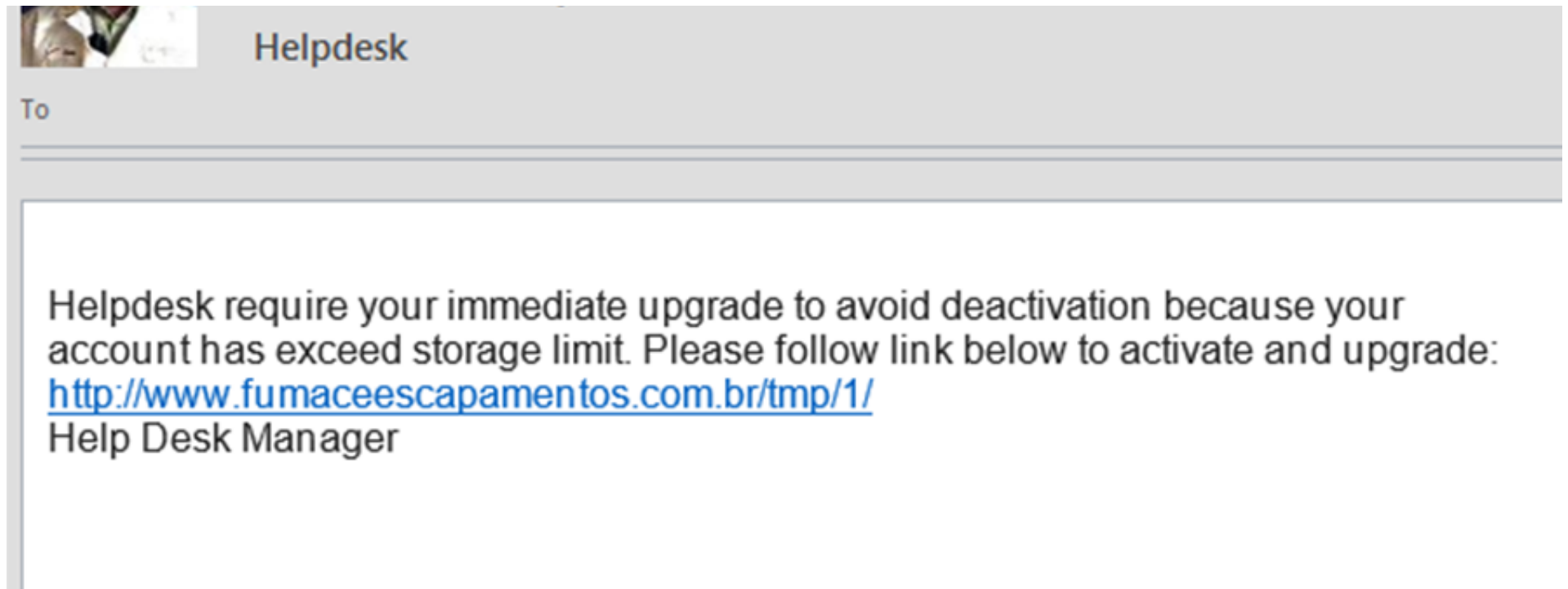
when you register for 2 years or more. 1st year price \$1.00 Additional years \$19.99

~~\$14.99*~~ **\$2.99***

when you register for 2 years or more.
1st year price \$2.99 Additional years \$14.99

Select

HOW ARE THEY GETTING IN?



- Obvious grammatical errors
- Missing email signatures
- Suspicious attachments or links
- Requests for money or account information

SOCIAL ENGINEERING

SOCIAL ENGINEERING

- Social Media
- Telephone
- Thumb Drives
- Con Artists



SOCIAL ENGINEERING CASE STUDY

HOMELAND SECURITY – A CASE STUDY

THE TEST

- 60% of generic drives
- 90% of branded drives



IF YOU ARE BREACHED

CRIME



WHAT IF YOU ARE BREACHED?

- Adhere to HIPAA reporting rules
- Report to insurance
- If bank related, contact your financial institution immediately
- Report it at www.ic3.gov
- Contact your local FBI office
- Gather all evidence
 - *Emails including headers*
 - *Wiring instructions*

FBI – OMAHA CYBER SQUAD

CYBER TASK FORCE (CTF)

- Douglas County Sheriff's Office
- Omaha Police Department
- Nebraska State Patrol
- Sarpy County Sheriff's Office
- Iowa Division of Criminal Investigation
- FBI Agents
- Analysts
- Computer Scientist
- CART personnel (forensics)



INTERNAL THREAT CHECKLIST

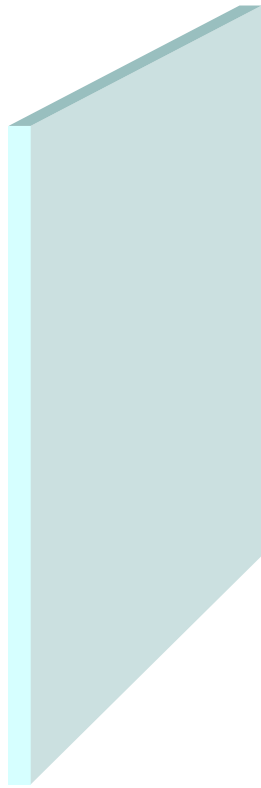
WHAT CAN YOU DO?

- ☐ Educate, Educate, Educate – first line of defense
- ☐ Get Tested (Security Assessments)
- ☐ Respect Test Results (physical and cyber)
- ☐ Adhere to Rotation of Duties / Change control policies
- ☐ Respect Termination Policies
- ☐ Respect Mobile Devices and Removable Media for what they have on them
- ☐ Report, Report, Report – Make it acceptable to report
- ☐ Define the threat – What are you trying to protect?
- ☐ Analyze the organization's culture and determine potential risks

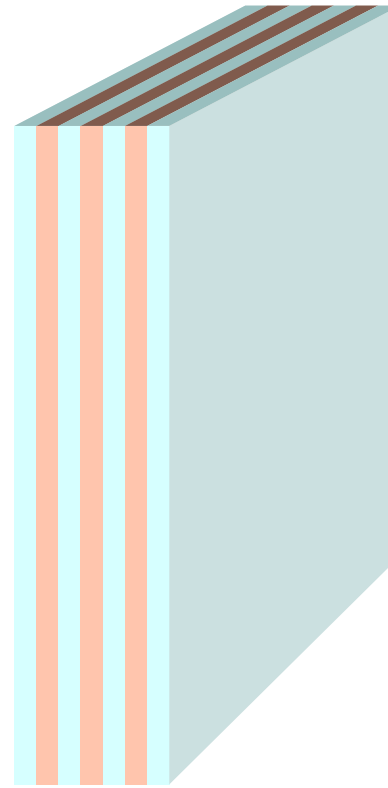
SECURITY IS A SHARED RESPONSIBILITY

- Company initiative and buy in
- Baseline security assessment
- Security is a Group Effort and is dependent on people
- SPEAK UP! – Don't be afraid to ask questions and report unsafe activity

MITIGATE THE EXTERNAL THREAT



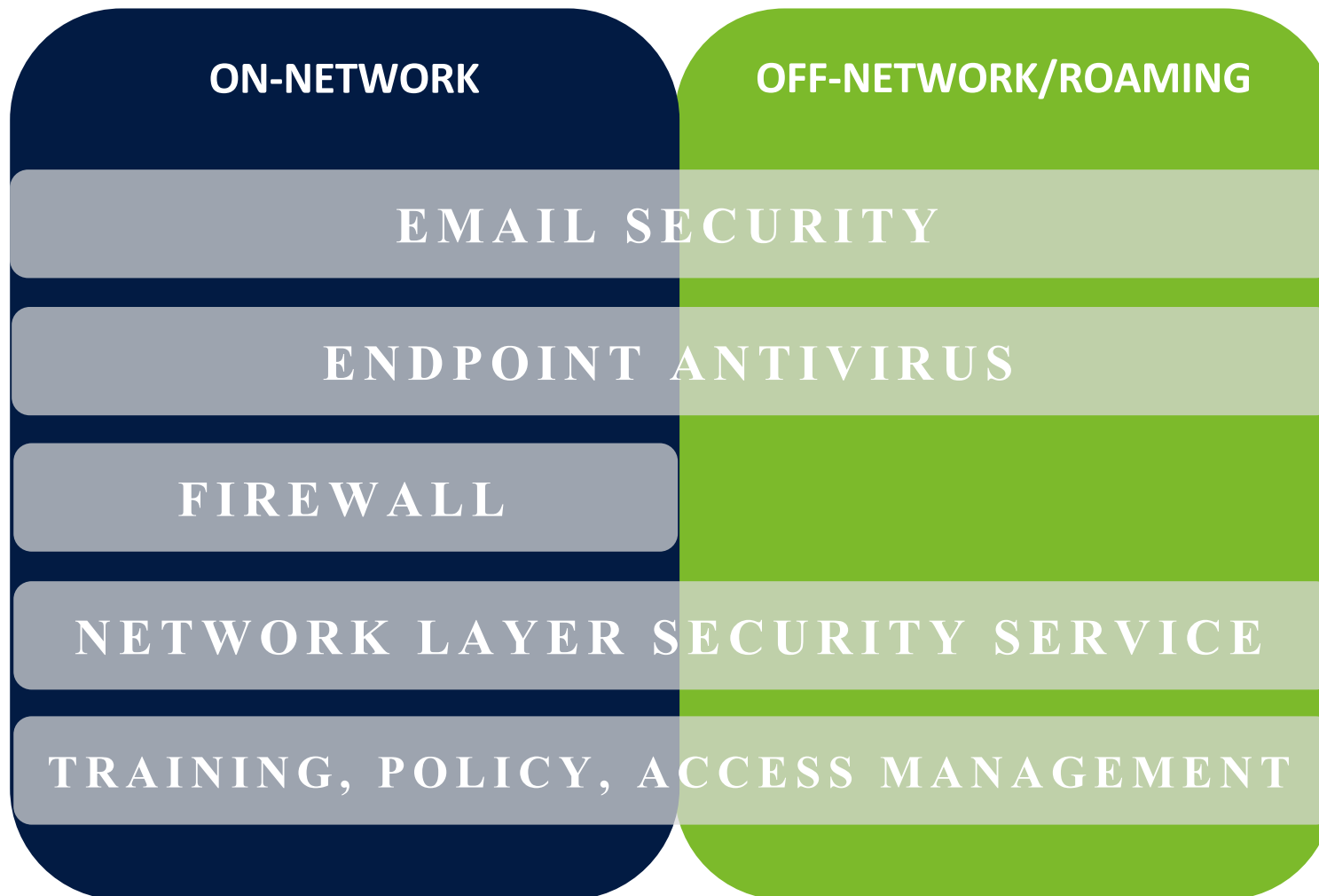
**NORMAL
GLASS**



**BULLET
PROOF
GLASS**
consisting of
normal glass (blue)
and polycarbonate
(red) layers

MITIGATE THE EXTERNAL THREAT

SECURITY IS ABOUT MANAGING RISK THROUGH LAYERS



EXTERNAL THREAT CHECKLIST

- ☐ **Identify security needs and risks**
- ☐ **Begin with the basics**
 - *Strong passwords, antivirus, antispyware, intrusion prevention systems, encryption technologies, firewalls, content filtering, secure wireless access points*
- ☐ **Keep your systems updated (patching)**
 - *Adhere to regular software and system patching schedules*
- ☐ **Backup**
 - *Perform regular backups and test restores*
- ☐ **Educate employees**
 - *Adopt a formal policy*
- ☐ **Keep devices safe from physical theft**
- ☐ **Encrypt data at rest**
- ☐ **Don't mix business and family**
- ☐ **Secure your websites**
- ☐ **GET EXTERNAL HELP**

PERSONAL AND FAMILY SECURITY

- ☐ Utilize strong passwords and change them frequently
- ☐ Secure email with spam filters
- ☐ Virus Protection - Install anti-virus / anti-malware software
- ☐ Secure your wireless network (don't broadcast SSID)
- ☐ Download the latest patches
- ☐ Perform regular backups
- ☐ Mobile Device Security (pins, screen locks, biometrics, restrictions, encryption)
- ☐ Think before you click
- ☐ Use Common Sense
- ☐ Subscribe to Identity Protection / Credit Monitoring Services
 - *American Express Credit Secure*
 - *LifeLock*

IS YOUR PASSWORD LISTED?

TOP 20 MOST COMMON PASSWORDS

(as a percentage of all passwords)

1. 123456	4.1%	11. login	0.2%
2. password	1.3%	12. welcome	0.2%
3. 12345	0.8%	13. loveme	0.2%
4. 1234	0.6%	14. hottie	0.2%
5. football	0.3%	15. abc123	0.2%
6. qwerty	0.3%	16. 121212	0.2%
7. 1234567890	0.3%	17. 123654789	0.2%
8. 1234567	0.3%	18. flower	0.2%
9. princess	0.3%	19. passw0rd	0.2%
10. solo	0.2%	20. dragon	0.1%

SUMMARY

- Protecting your business starts by understanding the internal and external technology threats
- Start by assessing your current environment and creating an IT security plan
- Dedicate time and resources to execute IT security plan

Q&A

SECURITY STORIES IN THIS ROOM?

- Anyone willing to speak up?

INVERSE Q&A

- Discuss with the person next to you
- For you, what was the key take-away from the session?
- What might you do differently going forward?

TRADITIONAL Q&A

CONTACT

SCOTT KROEGER

LUTZ TECH

SKROEGER@LUTZ.US

402.827.2304