Cybersecurity – Protecting your Resident's Data – Oversight over Information Technology

Ben Hunter III, CISO
CPA/CITP, CISA, CRISC, CDPSE, CISM

Bernard Robinson & Company

Virginias
COUNCIL FOR AFFORDABLE AND RURAL HOUSING

0

Ben Hunter III, CISO
CPA/CITP, CISA, CRISC, CDPSE, CISM

Bernard Robinson & Company

Background

- Eagle Scout
- Served two-year mission in Portugal for the Church of Jesus Christ of Latter-day Saints
- Married 21 years – 4 children
- United States Marine Corps
- Bachelor of Science in Accounting from UNC Greensboro
- Master of Science in Accounting from UNCG Greensboro
- Chief Information Security Officer at BRC
- Senior Risk Advisory Manager at BRC CPA.
- Specializes in Cybersecurity, SOC Reports and Information Technology Audits and Assessments.

1

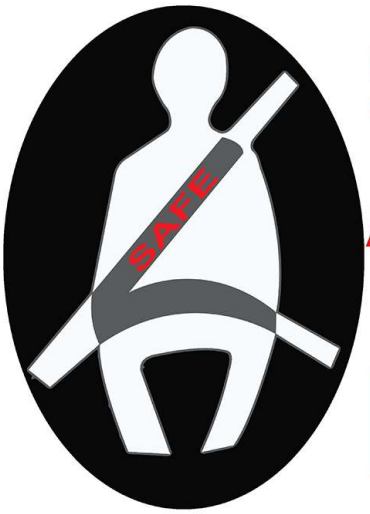
Disclaimer

This presentation has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice.

Objectives

- Understand that cybersecurity is for everyone and should become a habit
- Understand why we should care about cybersecurity and the data that is at risk
- Understand why we should train our employees
- Understand why we should have a cyber risk assessment annually
- Understand the ransomware risk
- Understand why we need to verify backups and restore capabilities
- Understand the danger of phishing and how phishing simulation reports can help
- Understand common Phishing Red Flags
- Understand the importance of network security monitoring
- Understand what is a vulnerability scan and how it helps
- Understand the importance of oversight over IT
- Understand what to do when there is a breach
- Understand how to create a good password
- Understand why USBs and USB ports are dangerous
- Understand how important 2FA / Multi-Factor Authentication is

Compliance – Security - Safety



Seatbelts
Are
For
Everyone

SERVING CLIENTS ACROSS THE SOUTHEAST

4

4

Why should you care – Personally or Professionally

https://www.rd.usda.gov/files/hb-2-3560.pdf

HB-2-3560 MFH ASSET MANAGEMENT HANDBOOK

Rural Development Handbooks - Internal Control over Financial Reporting

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the Partnership's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the Partnership's financial statements that is more than inconsequential will not be prevented or detected by the Partnership's internal control.

IT General Controls are part of this Internal Control over Financial Reporting

SERVING CLIENTS ACROSS THE SOUTHEAST

5

5

What are Information Technology General Controls

The most common ITGCs:

- Logical access controls over infrastructure, applications, and data.
- System development life cycle controls.
- Program change management controls.
- Data center physical security controls.
- System and data backup and recovery controls.
- Computer operation controls.

Data at Risk

- Social security number
- Dates of birth
- Addresses
- Email addresses
- Bank account information
- Client / Customer data
- Intellectual property
- Physical & Financial Assets
- Payroll information
- Corporate information

Data at Risk –

From the HB-2-3560 MFH ASSET MANAGEMENT HANDBOOK

Tenant Data: Composition of Family_____
Tenant/Family/Elderly/Handicapped_____
Unit-Size Eligibility_____
Last Verified Income _____ as of _____
RA: _____
Section 8 Voucher: _____
Current Security Deposit: _____

Train Your Employees – HUD Requirement

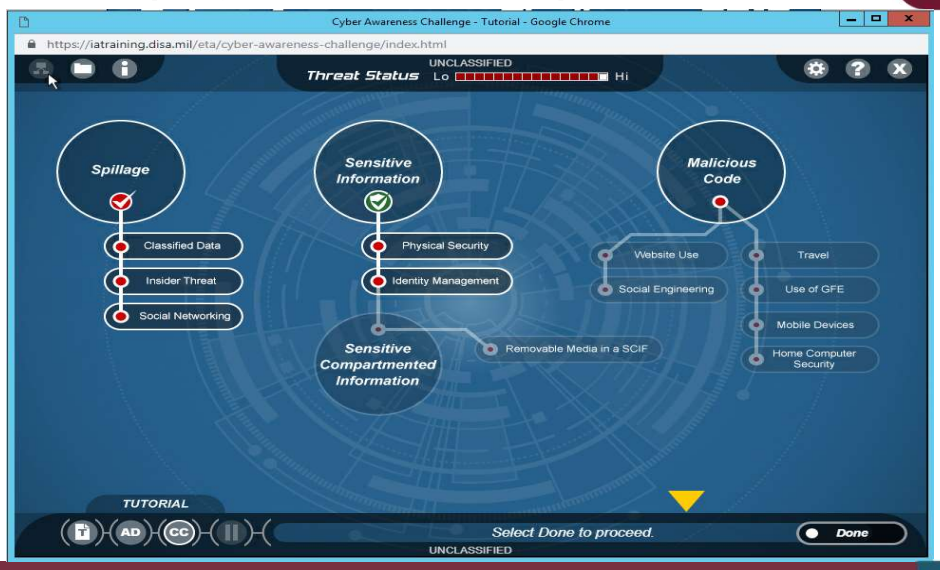
From the HUD Website:

The CyberAwareness Training described above is the same training required for those individuals who transmit TRACS files. If the training has been completed to satisfy TRACS security training requirements, this will satisfy EIV security training requirements as well so long as the completion date represented on the *Certificate of Completion* is not older than one year.

To complete online FREE Security Awareness Training:

- Open your web browser.
- https://iase.disa.mil/eta/Pages/online-catalog.aspx
- https://iatraining.disa.mil/eta/cyber-awareness-challenge/launchPage.htm
- Press Enter. This should open to the new CyberAwareness Challenge (unclassified) 2019.
- Choose Start/Continue CyberAwareness Challenge Department of Defense Version
- Proceed with the training.

Train Your Employees – HUD Requirement



Cyber Risk Assessment

- Know what data is at risk and what is your CRITICAL data.
- Know where the data is located on your network – servers, file shares, applications, cloud applications, local laptops.
- Know your risk tolerance – how long could you be without your data and still have a viable business.
- Know or verify what controls and security measures you already have in place.

12

NIST Cybersecurity Framework

What processes and assets need protection	Identify
What safeguards are available	Protect
What techniques can identify incidents	Detect
What techniques can minimize the impact of incidents	Respond
What techniques can help us recover	Recover

13

3 ways to recover from Ransomware:

1. Pay and Pray
2. Restore from backups
3. Forensically find the malware, destroy it and re-create your files

14

Phishing - Business Email Compromise

70% of cyberattacks use a combination of Phishing and hacking.

Phishing emails include fake notifications from banks, e-payment systems, email providers, social networks, online games, etc.

Cybercrime makes criminals more money than drugs.

Would you care if someone hacked your email account, but did nothing but watch?

15

Phishing Red Flags

- From
- To
- Date
- Subject
- Attachments
- Content
- Hyperlinks

The list contains different parts of an email that contain clues that will indicate the email is a phishing attempt. The seven slides that follow will detail the clues you need to look for.

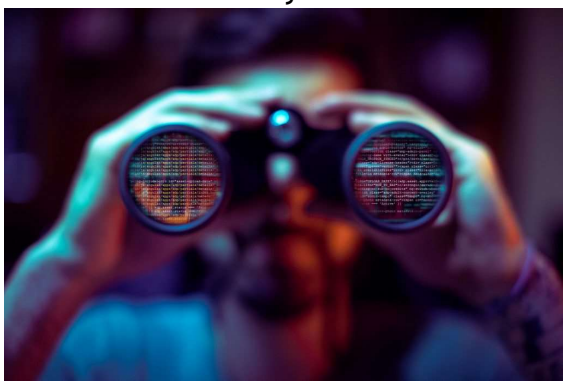
Remember: If it seems weird, or doesn't make sense, STOP and think about the situation.

Phishing - Business Email Compromise

- Don't trust anyone
- Never click on links in email and some website ads are compromised as well
- Always go to the website by opening a new browser window and typing in the URL
- Use 2 factor authentication
- Pay attention to patterns
- Provide training to everyone in the organization – Not just once a year

Network Security Monitoring

- 24/7 Managed Detection & response
- Continuously monitor your cyber assets to detect threats and vulnerabilities which may have bypassed other security controls
- Real-time threat intelligence
- User behavior analytics
- Monitored SIEM
- Monitored Firewall

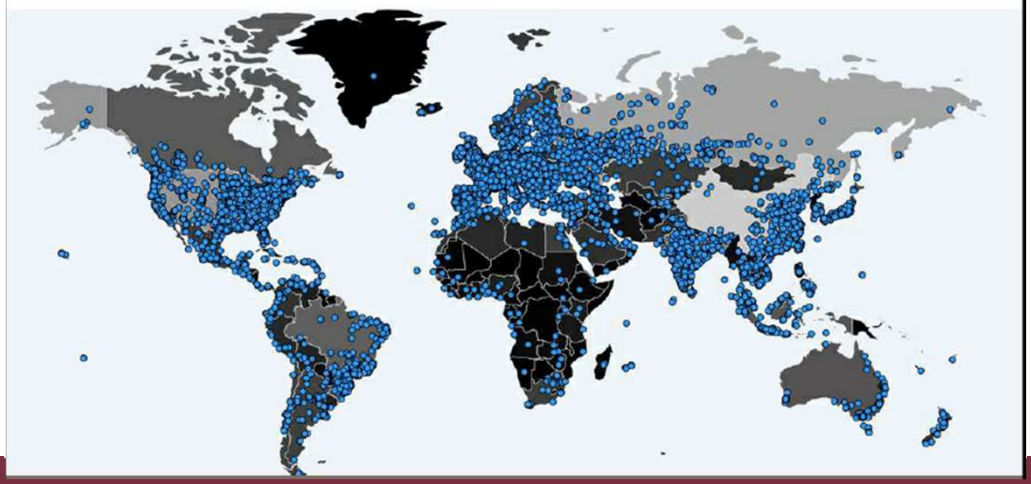


SERVING CLIENTS ACROSS THE SOUTHEAST

18

18

Every blue dot represents a wannacry ransomware infection that occurred between 10:30am CST on 5/12 and 2:30 CST on 5/15/17.



WannaCry – Ransomware attack in **MAY** 2017. Patch issued in **MARCH** 2017!!!!
COMPLETELY AVOIDABLE

19

19

Vulnerability Scanning and Patching

- Designed by humans
- Move fast and break stuff
- Vulnerabilities are constantly found
  - 14712 found in 2017
  - 16555 found in 2018
  - 3261 found as of 5/2/2019
- Scan your systems using Qualys or Nessus to find known vulnerabilities
- Risk rank the vulnerabilities found
- FIX THEM – PATCH YOUR SYSTEMS

Vulnerability Scan Reports

Summary of Vulnerabilities

Vulnerabilities Total	1580 (+216)	Security Risk (Avg)	4.9

by Status

Status	Confirmed	Potential	Total
New	1306	-	1306
Active	274	-	274
Re-Opened	0	-	0
Total	1580	-	1580
Fixed	8	-	8
Changed	1314	-	1314

by Severity

Severity	Confirmed	(Trend)	Potential	(Trend)	Information Gathered	Total	(Trend)
5	677	(0) -	-		-	677	(+115)
4	903	(0) -	-		-	903	(+101)
3	0	(0) -	-		-	0	(0) -
2	0	(0) -	-		-	0	(0) -
1	0	(0) -	-		-	0	(0) -
Total	1580	(0) -	-		-	1580	(+216)

5 Biggest Categories

Category	Confirmed	(Trend)	Potential	(Trend)	Information Gathered	Total	(Trend)
Local	941	(0) -	-		-	941	(+155)

Vulnerability Scan Reports

IP	DNS	NetBIOS	OS	IP Status	QID	Title	Type	Severi	Po	Protoc	FQE	SSL	CVE ID	Vendor Reference
			Windows 2008 R2 Standard Service Pack 1	host scanned, found vuln	38603	SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)	Vuln	3	1433	tcp		over ssl	CVE-2014-3566	POODLE
			Windows 2008 R2 Standard Service Pack 1	host scanned, found vuln	19824	Microsoft SQL Server Database Link Crawling Command Execution - Zero Day	Practice	3						
			Ubuntu / Fedora / Tiny Core Linux / Linux 3.x	host scanned, found vuln	70008	NetBIOS Name Conflict Vulnerability	Vuln	3					CVE-2000-0673	MS00-047
			Ubuntu / Fedora / Tiny	host scanned, found vuln	70009	NetBIOS Release Vulnerability	Vuln	3					CVE-2000-0673	MS00-047

Threat	Impact	Solution	Exploitability	Associated Malware
The SSL protocol 3.0 design error, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attacks.	An attacker who can take a man-in-the-middle (MitM) position can exploit this vulnerability and gain access to encrypted communication between a client and	Disable SSLv3 support to avoid this vulnerability. Examples to disable SSLv3. nginx: list specific allowed protocols in the "ssl_protocols"	Source: Metasploit Reference:CVE-2014-3566 Description:HTTP SSL/TLS Version Detection	
Microsoft SQL Server is exposed to a remote command execution vulnerability.	Successful exploitation could allow attackers to obtain sensitive information and execute arbitrary code.	There are no solutions available at this time.	Source: Qualys Reference:CVE-0000-0000 Description:Microsoft SQL Server - Database Link	
A malicious user can send a NetBIOS Name Conflict message to the NetBIOS name service even when the receiving machine is not in the process of registering its	If successfully exploited, this vulnerability could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.	The best workaround for Microsoft Windows and Samba Server is to block all incoming traffic from the Internet to UDP ports 137 and 138.	Source: The Exploit-DB Reference:CVE-2000-0673 Description:Microsoft Windows NT 4.0/2000 -	
A malicious user can send a NetBIOS Release message to a NetBIOS name service.	If successfully exploited, the receiving machine is forced to place its name in conflict so that it will no longer be able to use it.	This is the correct protocol behavior. The best workaround for Microsoft Windows and Samba servers is to block all incoming traffic from the Internet to UDP ports 137 and	Source: The Exploit-DB Reference:CVE-2000-0673 Description:Microsoft Windows NT 4.0/2000 -	
A vulnerability in the Secure Sockets Layer (SSL) VPN	An attacker could exploit this vulnerability by sending	Patch:	Source: The Exploit-DB	

SERVING CLIENTS ACROSS THE SOUTHEAST

22

22

Oversight over IT

- What oversight do you have over IT?
- Get your email, access your applications – IT is going great, right?
- Do you review contracts with your outsourced IT?
- Do you have a statement of work or service agreement with your IT?
- Do you receive any status reports?
  - Firewall and system uptime, penetration attempts blocked, user logins, websites visited by employees, list of websites or genres of websites blocked
- System updates / patching reports?

SERVING CLIENTS ACROSS THE SOUTHEAST

23

23

What to do when there is a breach

- Consult with an attorney!
- Mitigate the damage - shut down ports so data stops flowing out, turn off servers, take them offline, etc.
- Identify the data accessed and retrieve it or prevent its spread.
- Communicate - but control the vocabulary. Customers want to hear about your breach from you, not the news.
- Patch the point of entry.
- Bring in an outside forensic investigation team.
- Attorney's and forensic teams can be expensive, but so can the fines and continued data loss without them.

Security Versus Usability

Worst Passwords of 2021

1. 12345
2. 123456
3. 123456789
4. test1
5. password
6. 12345678
7. zinch
8. g_czechout
9. asdf
10. qwerty
11. 1234567890
12. 1234567
13. Aa123456.
14. iloveyou
15. 1234
16. abc123
17. 111111
18. 123123
19. dubsmash
20. test
21. princess
22. qwertyuiop
23. sunshine
24. BvtTest123
25. 11111
26. ashley
27. 00000
28. 000000
29. password1
30. monkey
31. livetest
32. 55555
33. soccer
34. charlie
35. asdfghjkl
36. 654321
37. family
38. michael
39. 123321
40. football

Authentication - Password Tips

Even if you are using a “strong, complex” password, the hackers know our “trick”

Swimming = Sw1mm!ng46 Sw1mm!ng47

You can spend $3000 on a computer that can crack all 9 character passwords in 1.5 days. That is every password combination possible using 9 characters. It generated 1.5 billion passwords per second.

Authentication - Password Tips

Per NIST – passphrases are now recommended.

Minimum Length = 10 characters, but NIST is asking for companies to allow up to 64 characters. The **longer** the better.

No longer recommended to change your password every 30 or 90 days. Change your password when you think it has been compromised.

SERVING CLIENTS ACROSS THE SOUTHEAST

28

28

Passphrase example

GreenSpatulabreakfastbagelSunlight

Gr3enSp@tulabr#akf@stbagelSunl!ght

SERVING CLIENTS ACROSS THE SOUTHEAST

29

29

Passphrase - more good news

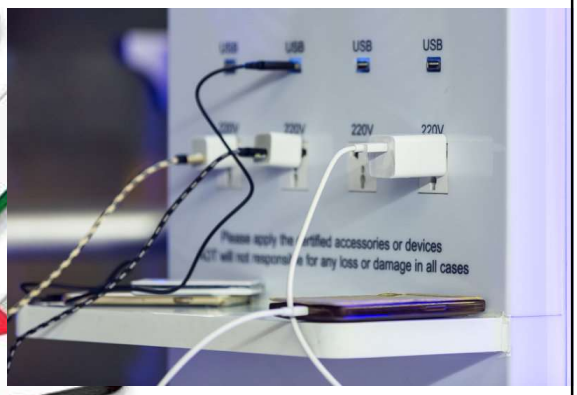
Use encryption software on your Phone
Use online password manager
Lock the paper in your safe

Write them down

SECURELY

30

USB ports/ Flash drives



31

Cyber Tips for EVERYONE

Don't trust anyone – secure your physical device.
Use a code on your phone or don't store sensitive data on your phone.
Don't trust anything you find – flash drive, phone, etc.
Don't trust communal workstations – there could be keylogger software on it.
Use Popup blockers on browsers, erase cookies.
Don't store (remember me) passwords on the web OR
use the same password for multiple sites.
Never go to a banking site, or enter a password on an unsecure network.
Use 2 factor authentication - (Gmail example).
!!!!!!!!!USE STRONG PASSWORDS!!!!!!!!
Keep your devices up to date. Yes – update your software and apps.
Yes – use antivirus / anti-malware software.
Monitor your credit and Identity. LifeLock, Identity Guard, etc.
Be careful on Social Media – don't post personal information, don't click on links.
DON'T TAKE COMPROMISING PHOTOS – or store them on the cloud.
Don't use free Wi-Fi – or use a VPN service.
Disable the automatic Wi-Fi connectivity on your devices – and delete Wi-Fi you aren't using regularly.
Don't use Torrent websites – Bit Torrent is a technology used to distribute files over the internet.

32

Foundational Actions

1. Make sure your backups work and are as current as you can afford.
2. Train your employees (and yourself) more than once a year.
3. Keep a security mindset. If something appears off or out of pattern, slow down, investigate, switch to analog (a phone call).
4. Use long passphrases AND two-factor authentication everywhere possible.
5. Have your system scanned for vulnerabilities at least every 6 months, risk rank the vulnerabilities and get them fixed.
6. Get a managed security monitoring provider.

33

Questions

Please don't hesitate to ask

Bernard Robinson & Company

SERVING CLIENTS ACROSS THE SOUTHEAST

34

Objectives

- Understand that cybersecurity is for everyone and should become a habit
- Understand why we should care about cybersecurity and the data that is at risk
- Understand why we should train our employees
- Understand why we should have a cyber risk assessment annually
- Understand the ransomware risk
- Understand why we need to verify backups and restore capabilities
- Understand the danger of phishing and how phishing simulation reports can help
- Understand common Phishing Red Flags
- Understand the importance of network security monitoring
- Understand what is a vulnerability scan and how it helps
- Understand the importance of oversight over IT
- Understand what to do when there is a breach
- Understand how to create a good password
- Understand why USBs and USB ports are dangerous
- Understand how important 2FA / Multi-Factor Authentication is

SERVING CLIENTS ACROSS THE SOUTHEAST

35

35

Thank You

for your attention!

Bernard Robinson & Company

SERVING CLIENTS ACROSS THE SOUTHEAST

36

37