

The logo for Elliott Davis, consisting of the words "elliott davis" in a white, lowercase, sans-serif font, set against a solid orange rectangular background.

Data Security and Cyber Threat Update



Jimmy Buddenberg
*Risk Advisory &
Cybersecurity
Practice Leader*

1

The logo for Elliott Davis, consisting of the words "elliott davis" in a white, lowercase, sans-serif font, set against a solid orange rectangular background.

Disclaimer

This material was used by Elliott Davis during an oral presentation; it is not a complete record of the discussion. This presentation is for informational purposes and does not contain or convey specific advice. It should not be used or relied upon in regard to any particular situation or circumstances without first consulting the appropriate advisor. No part of the presentation may be circulated, quoted, or reproduced for distribution without prior written approval from Elliott Davis.

2

Cybersecurity Advisory Services

Securing Where You Want To Be

Elliott Davis Cybersecurity Advisory consultants work with customers to reduce their overall risk and impact of a cyber-attack by performing risk assessments, penetration tests, and architectural reviews. Consultants also evaluate the effectiveness of policies and procedures and can assist in the development and testing of incident response plans.



3

The Elliott Davis logo, consisting of a stylized circular icon and the text "elliott davis", is contained within an orange rectangular box.

Lesson #1

We Are All A Target

4

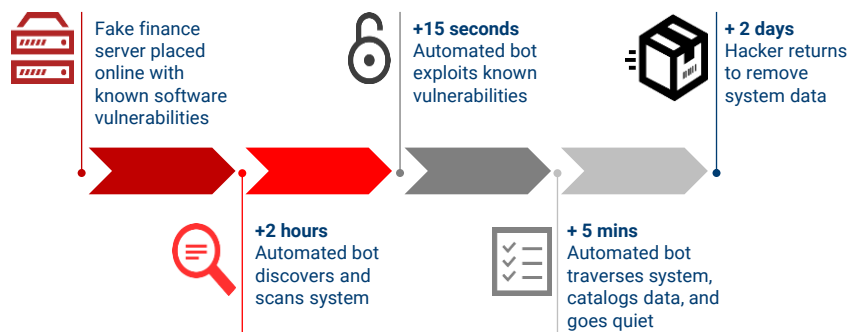
Polling Question #1

5

How Some Targets are Acquired by Criminals

Attacks are initially driven through automated 'bots' which either automate spam messages or scan the internet for vulnerabilities and carry out large portions of cyber attacks without any human interaction.

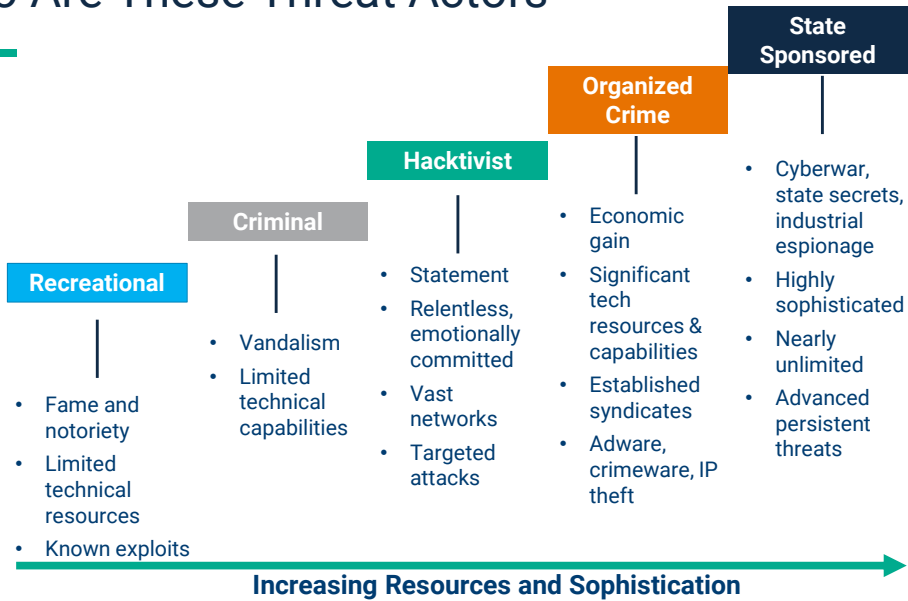
Live Security Test Performed



 **elliott davis**

6

Who Are These Threat Actors



7

Impact on the Public Sector – A Shift is Occurring

- Out of 21 industries, Public has the **second highest** number of incidents behind Professional Services.
- Out of 21 industries, Public has the **fifth highest** number of data breaches.
- The vast majority of incidents on public sector were a result of **malware**.
- Most data breaches on public sector are a result of **hacking** into a web application followed closely by **errors**.
- 59% of threat actors are **external** but an alarming 43% are **internal**. Last year the split was 75% external/30% internal.
- 75% of threat actor motivations are **financial**. Last year 29% of threat actor motivations were **financial** and 66% were **espionage**.

Frequency	6,843 incidents, 346 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Web Applications and Everything Else represent 73% of breaches.
Threat Actors	External (59%), Internal (43%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (75%), Espionage (19%), Fun (3%) (breaches)
Data Compromised	Personal (51%), Other (34%), Credentials (33%), Internal (14%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

Data provided from the Verizon 2020 Data Breach Investigations Report



8

elliott davis

Lesson #2

The Impact of Ransomware Continues to Rise

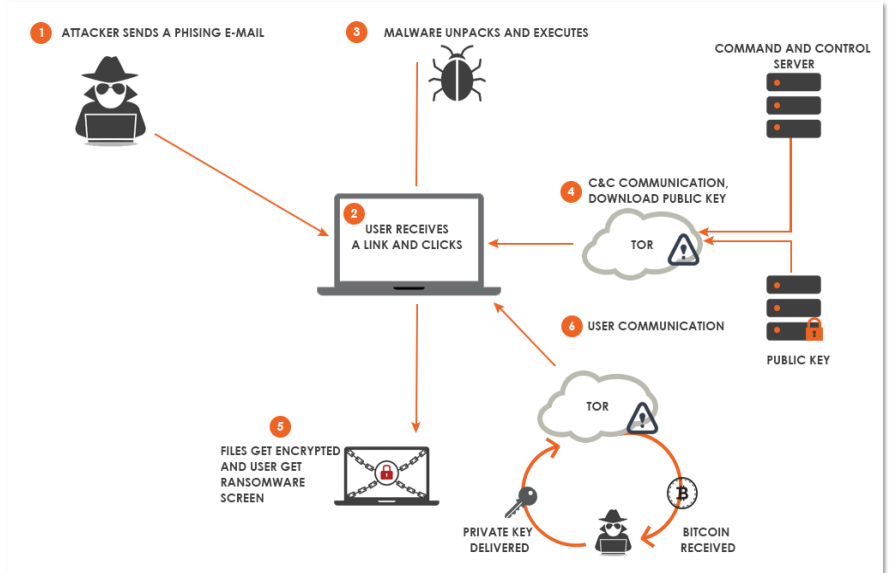
9

Polling Question #2

10

How Ransomware Works

76% of attacks typically happen during the night or on weekends



11

If You See This Screen.... Ugh

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm. Backups were either encrypted or deleted or backup disks were formatted. No free decryption software is available in the public. Do not rename the encrypted or informational text files. Do not move the encrypted or informational text files. This may lead to the impossibility of recovery of the certain files.

- Your reference ID: [REDACTED]
(we recommend to put the reference ID as the subject when contacting us)
- BTC wallet for payment: [REDACTED]

you can check the status here: [https://www.blockchain.com/btc/address/\[REDACTED\]](https://www.blockchain.com/btc/address/[REDACTED])

- Amount to pay (in Bitcoin): [REDACTED]
- Use chat in the right bottom of this page to contact us
We do not reply immediately, it may take a few hours for you to see first reply

To get the files in your network decrypted you should pay for the decryption software. The price for the decryptor is based on the network size, number of employees, annual revenue. Please feel free to contact us for amount of BTC should be paid.

You need to pack 2 pairs of files that is unique for you (somefile1.locked & somefile1.readme2unlock.bt and somefile2.locked & somefile2.readme2unlock.bt which have no sensitive information but only you own it) into ZIP and send to us.

And you'll have those 2 unlocked and would be sure it's working.

You should get in contact with us within 3 days after you noticed the encryption. If this doesn't happen the price is increased by 25% after 3 days.

The price would be increased by 50% in 1 week.

The price would be increased by 100% in 2 weeks (double price).

[REDACTED] Your network has been penetrated.

This link and your decryption key will expire in 21 days after your systems were infected. Sharing this link or email will lead to the irreversible removal of the decryption keys.

NO TIME remains for special price.

All files on each host in your network have been encrypted with flawless algorithm. Backups were either encrypted or deleted and backup disks were formatted. **There is no working decryption software that may solve this.** Do not rename the encrypted or informational text files. Do not move the encrypted or informational text files. This may lead to the impossibility of recovery of the certain files.

Also, we have gathered all your private sensitive data. So if you decide not to pay, we would share it. It may harm your business reputation.

Online chat

DopplePaymer Summer 2019

DopplePaymer Dec 2019



12

The Merging of Data Breach and Ransomware

Attention!

What happened?

We hacked your network and now all your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms. You cannot access the files right now. But do not worry. You have a chance to get it back! It is easy to recover in a few steps.

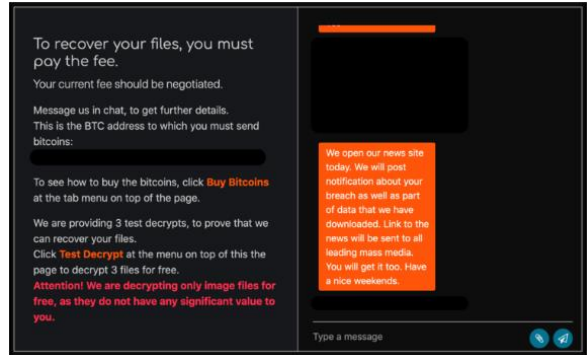
We have also downloaded a lot of data from your network, so in case of not paying this data will be released. If you dont believe we have any data you can contact us and ask a proof, also you can google [REDACTED]

When you pay us the data will be removed from our disks and decryptor will be given to you, so you can restore all your files.

How to contact us and get my files back?

The only method to restore your files and be safe from data leakage is to purchase a unique for you private key which is securely stored on our servers. To contact us and purchase the key you have to visit our website in a hidden TOR network.

Maze
Dec 2019



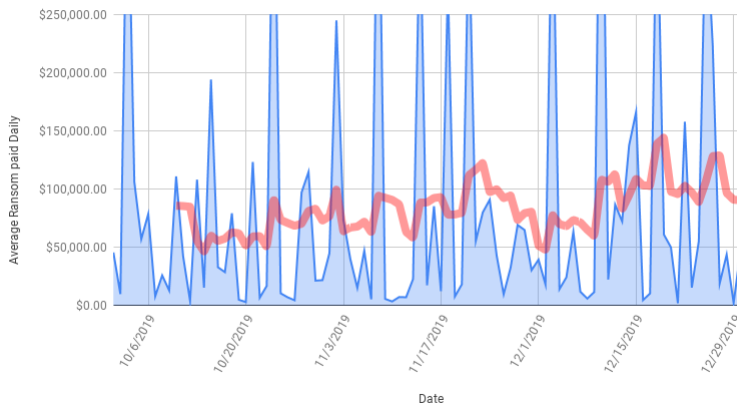
Maze
Dec 2019



13

Ransomware Payments on the Rise

Ransomware Amounts Paid Daily in Q4 2019

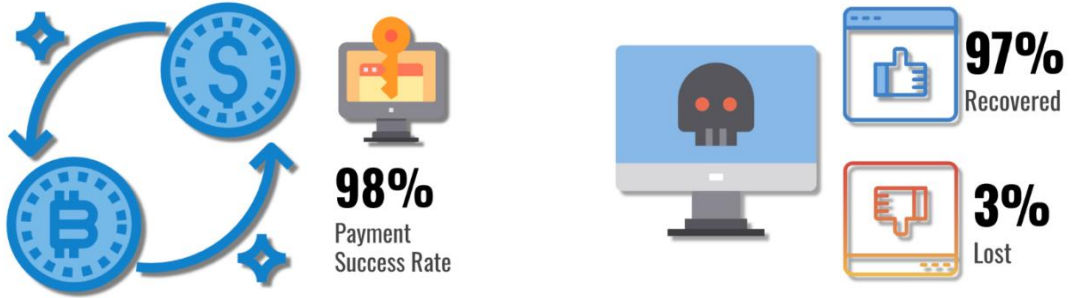


Data provided by Coveware



14

Do Criminals Provide the Keys...and Do They Work?

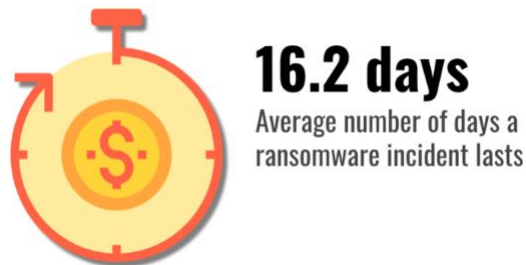


Data provided by Coveware

elliott davis

15

Ransomware Downtime



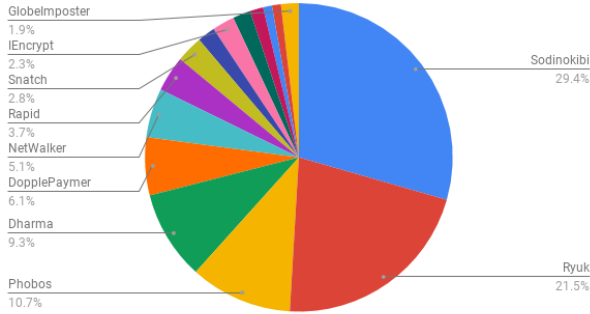
Data provided by Coveware

elliott davis

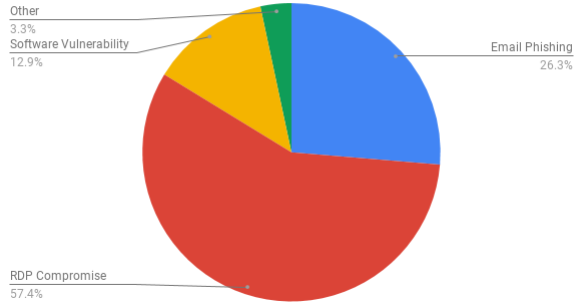
16

Ransomware Types and Their Attack Vectors

Ransomware Market Share by Type Q4 2019



Most Common Ransomware Attack Vectors Q4 2019



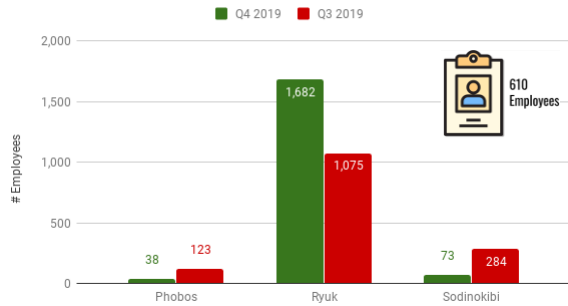
Data provided by Coveware



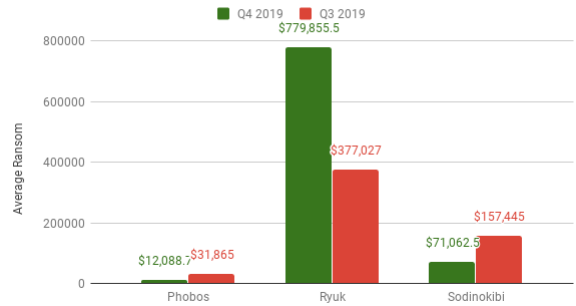
17

Ransomware Target Profile

Size of Victim Company by Number of Employees



Average Ransom Amount: Top 3 Ransomware Types



Data provided by Coveware



18

elliott davis

Lesson #3

Cybercriminals Will Kick You While You're Down

19

Polling Question #3

20

FBI Public Service Announcement – March 20, 2020

FBI SEES RISE IN FRAUD SCHEMES RELATED TO THE CORONAVIRUS (COVID-19) PANDEMIC

ALERT NUMBER: I-032020-PSA

Warns against:

- Fake CDC Emails
- Phishing Emails (charitable contributions, general financial relief, airline carrier refunds, fake cures/vaccines, fake testing kits)
- Counterfeit Treatments or Equipment

(We can expect a rash of phishing attacks related to the new stimulus bill that is in motion)

<https://www.ic3.gov/media/2020/200320.aspx>

 **elliott davis**

21

Forbes News...




 **elliott davis**

22

More Headlines...

Illinois Public Health Website Hit With Ransomware Amid Coronavirus

Hackers infected an Illinois Public Health provider website with ransomware during the coronavirus pandemic; Maze Team exploits, phishing, malware, and a PACS incident complete this week's breach roundup.



By Jessica Davis

HealthIT Security

WHO, coronavirus testing lab hit by hackers as opportunistic attacks ramp up

The World Health Organization has reportedly seen attempted cyberattacks double since the onset of the COVID-19 crisis, and a vaccine testing facility has also been targeted with ransomware.

By Nathan Eddy | March 24, 2020 | 10:58 AM



HealthIT Security

SECURITY today

HOME NEWS PRODUCTS MA

NPQY 2020 TRAINING CYBERSECURITY CAMPUS SECURITY & LIFE SAFETY DEAL

HHS.gov

I'm looking for...

Cyber Attack Hits Department of Health and Human Services Amid Government Coronavirus Response

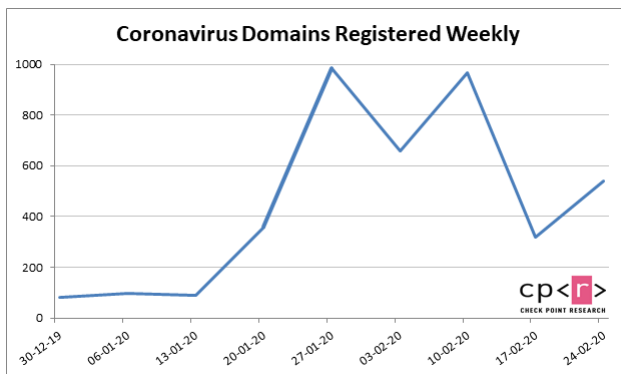
HHS officials said no personal data was accessed and the attack was not successful. But it could be a sign of things to come during the coronavirus pandemic.

By Haley Samsel | Mar 18, 2020



23

COVID-19 Domain Registrations



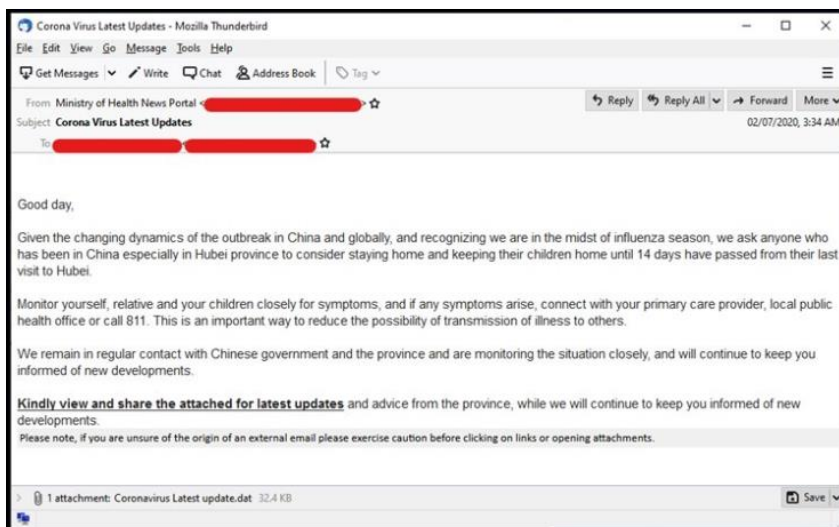
tneoronacure	today
coronacure	news
coronacure	pro
cocoronacuremedicalsupplies	com
coronacurealist	com
coronacurekits	com
coronacureprevention	com
viruscoronacure	com
coronacure	world
coronacure	store
coronacure	blog
coronacurenw	com
coronacurerecovery	com
coronacurevaccine	com

Out of these websites, **3%** were found to be malicious and an additional **5%** are suspicious.



24

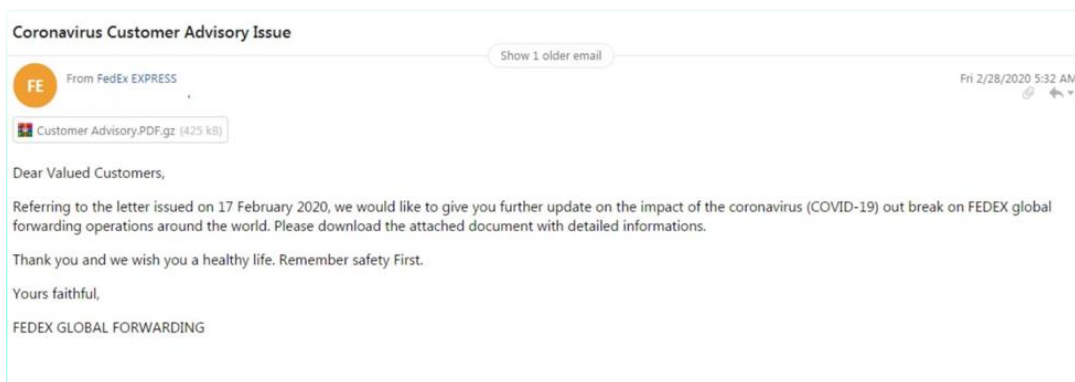
Sample Phishing Email



elliott davis

25

Sample Phishing Email



elliott davis

26

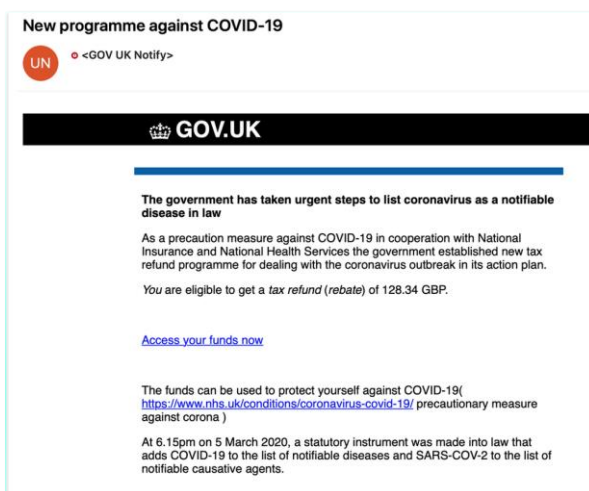
Sample Phishing Email



 **elliott davis**

27

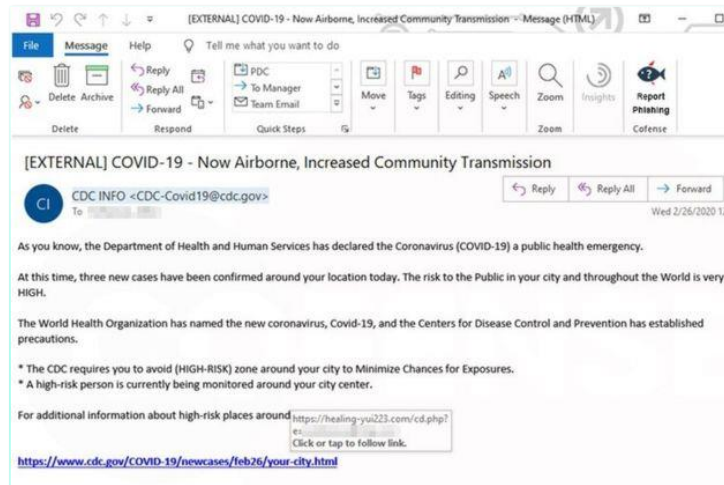
Sample Phishing Email



 **elliott davis**

28

Sample Phishing Email



 elliot davis

29

Phishing Recommendations

- Beware of online requests for personal information. Never respond to the email with your personal data.
- Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads.
- Watch for spelling and grammatical mistakes.
- Look for generic greetings. Phishing emails are unlikely to use your name. Greetings like “Dear sir or madam” signal an email is not legitimate.
- Avoid emails that insist you act now. Phishing emails often try to create a sense of urgency or demand immediate action.

 elliot davis

30

elliott davis

Lesson #4

Remote Workers Have Increased Your Risk

31

Polling Question #4

32

Collaboration Tools

- Remote collaboration tools can be extremely helpful to enable remote workers
- Internet trolls will look to join Zoom (or other) calls to display graphic content
- Suggestions
 - Require a password
 - Disable "join before host"
 - Control who enters the meeting
 - Monitor participants
 - Disable video



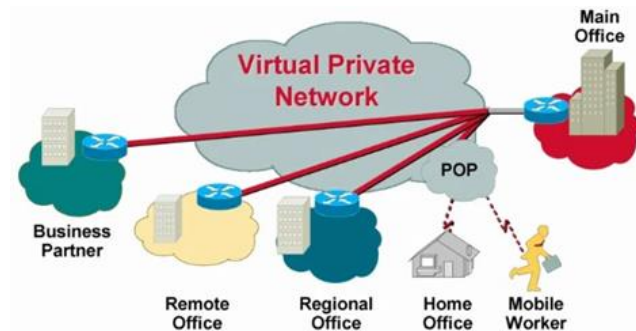
elliott davis

33

Virtual Private Networks (VPN)

Considerations when standing up a VPN

- Split tunneling
- VPN licenses
- VPN infrastructure
- VPN solutions
- Patching remote systems
- Users blurring the line between company and home networks
- User Awareness Training focused on the home network



elliott davis

34

Recommendations

35

Final Recommendations

- Secure any remote services to lower risk by **50%**. Audit/assess internet facing systems.
- Deploy multi-factor authentication on all administrative accounts to reduce risk by **40%**.
- Require multi-factor authentication for all remote access. If you rolled out VPN without it, its time to circle back and add it now.
- Use security awareness training tools to help employees identify social engineering techniques and spear-phishing emails with malicious links. Specifically add training in regards to phishing around coronavirus AND the new stimulus package.
- Perform offline backups and test data restoration ability.
- Perform a cyber program assessment.
- Perform web application penetration testing.

36

Ways to Measure Cyber Program Effectiveness

Program Assessment

CIS Control		Policy	Implementation	Reporting	Weighted Average	Grade
Basic	1 Inventory and Control of Hardware Assets	60%	77%	70%	75%	C
	2 Inventory and Control of Software Assets	56%	71%	72%	70%	C-
	3 Continuous Vulnerability Management	48%	59%	57%	58%	F
	4 Controlled Use of Administrative Privileges	79%	81%	85%	81%	B-
	5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	70%	87%	87%	85%	B
	6 Maintenance, Monitoring and Analysis of Audit Logs	63%	86%	83%	83%	B
Basic Controls - Results		63%	77%	76%	75%	C
Foundation	7 Email and Web Browser Protections	46%	60%	58%	58%	F
	8 Malware Defenses	53%	72%	72%	70%	C-
	9 Limitation and Control of Network Ports, Protocols, and Services	70%	87%	87%	85%	B
	10 Data Recovery Capabilities	100%	100%	93%	99%	A+
	11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	70%	93%	89%	90%	A-
	12 Boundary Defense	66%	80%	80%	79%	C+
	13 Data Protection	57%	52%	52%	53%	F
	14 Controlled Access Based on the Need to Know	63%	79%	79%	77%	C+
	15 Wireless Access Control	53%	69%	69%	67%	D+
	16 Account Monitoring and Control	67%	85%	84%	83%	B
Foundational Controls - Results		65%	78%	76%	76%	C
Organization	17 Implement a Security Awareness and Training Program	42%	66%	28%	60%	D-
	18 Application Software Security	67%	80%	79%	79%	C+
	19 Incident Response and Management	86%	77%	77%	78%	C+
	20 Penetration Tests and Red Team Exercises	28%	28%	28%	28%	F
Organizational Controls - Results		56%	63%	53%	61%	D-
Overall Grade		63%	75%	73%	74%	C

37

elliott davis

QUESTIONS?

We're here to help



Jimmy Buddenberg
Risk Advisory & Cybersecurity
Practice Leader
864.250.3936

VISIT

elliottdavis.com/covid19
elliottdavis.com/cyber

EMAIL

cyber@elliottdavis.com

38