Cyber Roundtable
October 2020

Next Roundtable

Tabletop Ransomware Simulation: Are you prepared?

Guest Speaker: Wes Spencer, CISO
Perch Security, former Chairman of FS-ISAC
with Mike Burgard and Jon Roberts

December 10, 2020 12:00 PM – 1:30 PM CT

www.marconet.com/events/tabletop-incident-response

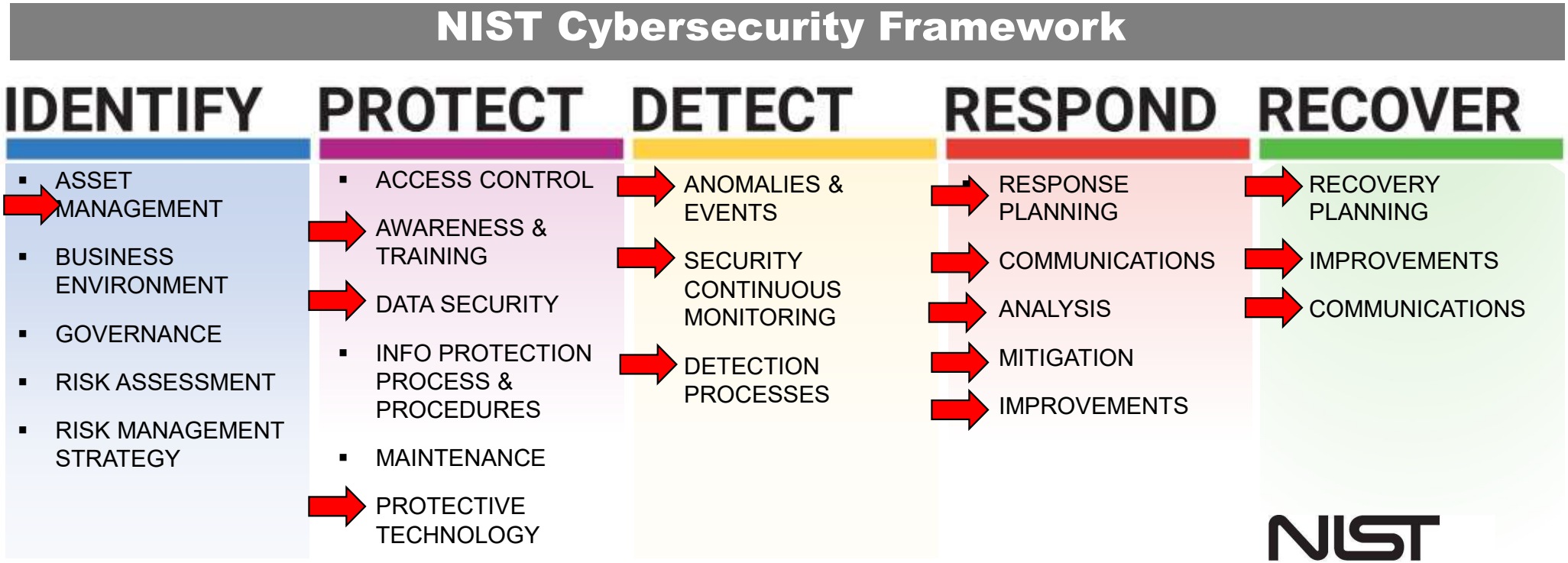
Agenda

What We See

Deep Dive

Taking Action

Cybersecurity Framework



- The NIST Cybersecurity Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

marco

Top Attacks in 2020

Phishing & Business Email Compromise

Up 650% since the start of COVID-19

RDP Exploits

Resurgence of older vulnerabilities

Ransomware

with ***Exfiltration of Data***

Work from Home Exploits

all of the above made easier plus more!

Not a great outlook…

On average

01	02	03	04
53% of attacks occur undetected.	Only 9% of alerts are correlated by SIEMs.	67% of data loss breaches are missed.	80% of tools are underused at default settings.

Source: FireEye/Mandiant 2020

Reality of Cyber Attacks

2019 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pha	114,702	Lottery/Sweepstakes/Inheritance	7,767
Non-Payment/Non-Delivery	61,832	Misrepresentation	5,975
Extortion	43,101	Investment	3,999
Personal Data Breach	38,218	IPR/Copyright and Counterfeit	3,892
Spoofing	25,789	Malware/Scareware/Virus	2,373
BEC/EAC	23,7	Ransomware	2,047
Confidence Fraud/Romance	19,473	Corporate Data Breach	1,795
Identity Theft	16,053	Denial of Service/TDoS	1,353
Harassment/Threats of Violence	15,502	Crimes Against Children	1,312
Overpayment	15,395	Re-shipping	929
Advanced Fee	14,607	Civil Matter	908
Employment	14,493	Health Care Related	657
Credit Card Fraud	14,378	Charity	407
Government Impersonation	13,873	Gambling	262
Tech Support	13,633	Terrorism	[illegible]
Real Estate/Rental	11,677	Hacktivist	39
Other	10,842		

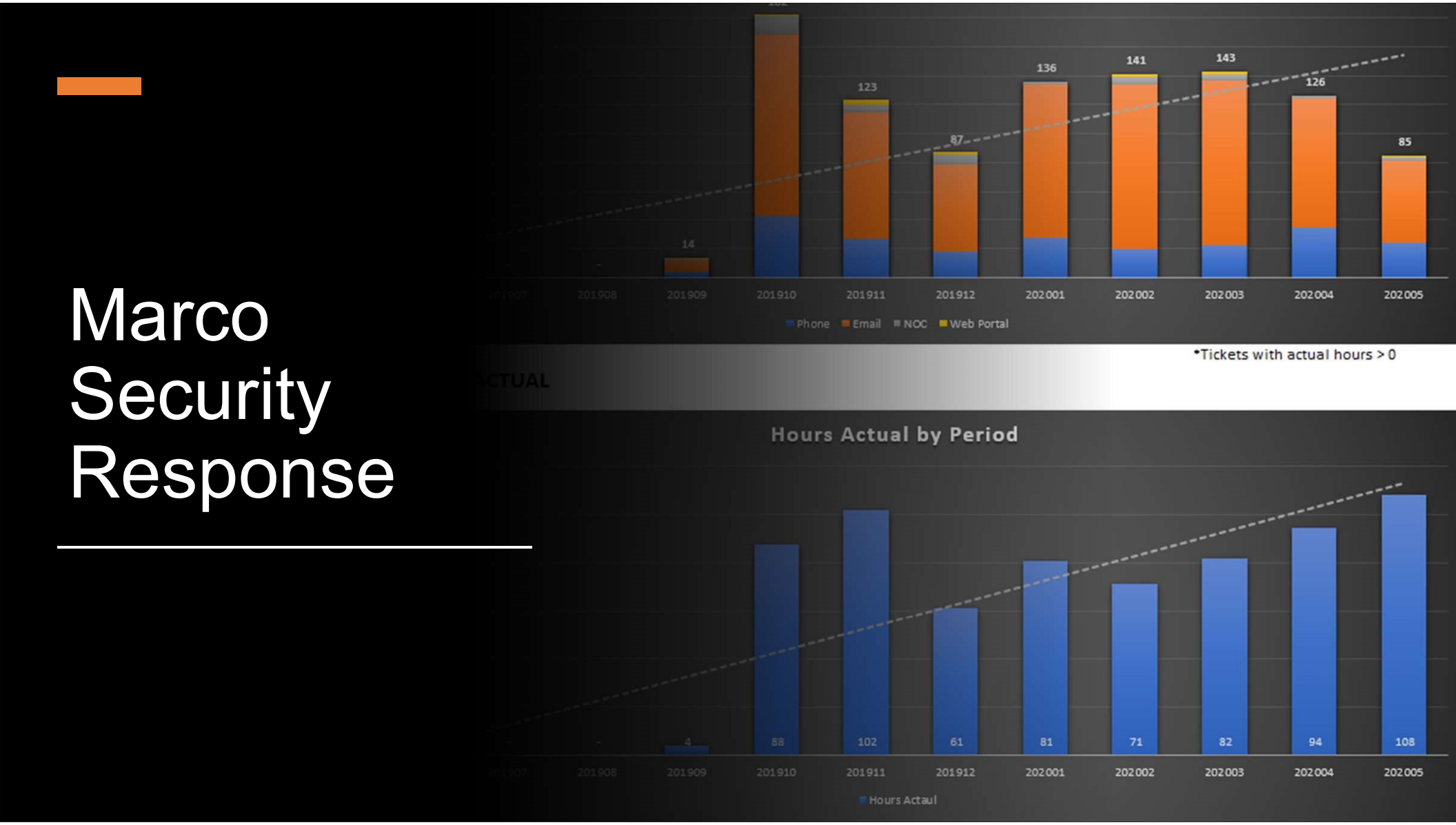
2019 Crime Types *Continued*

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,4	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

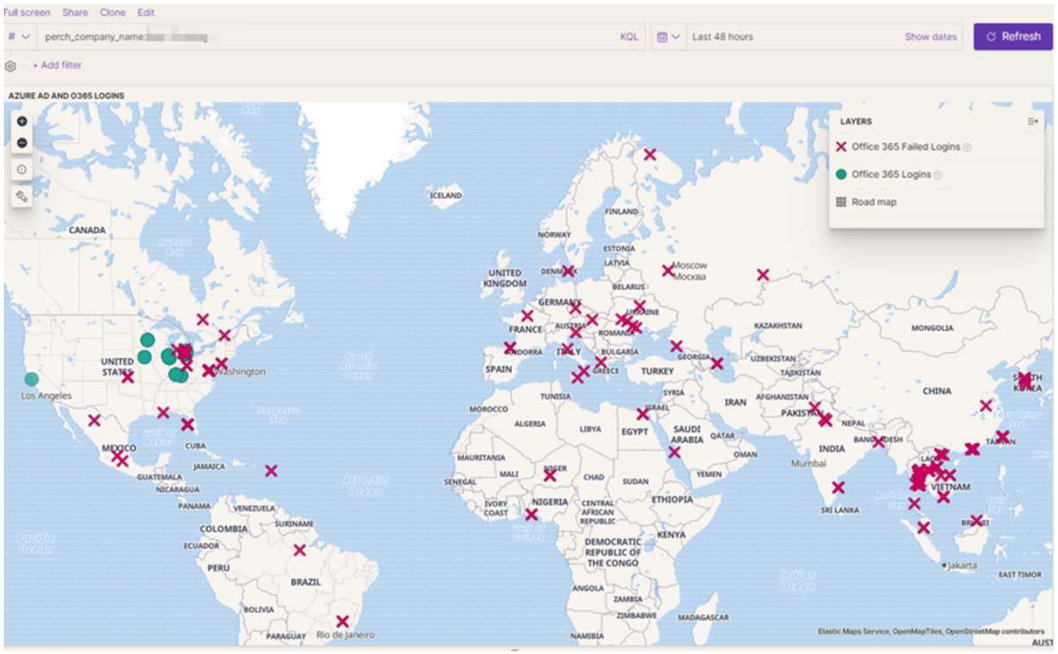
Source: IC3.gov

Marco Security Response



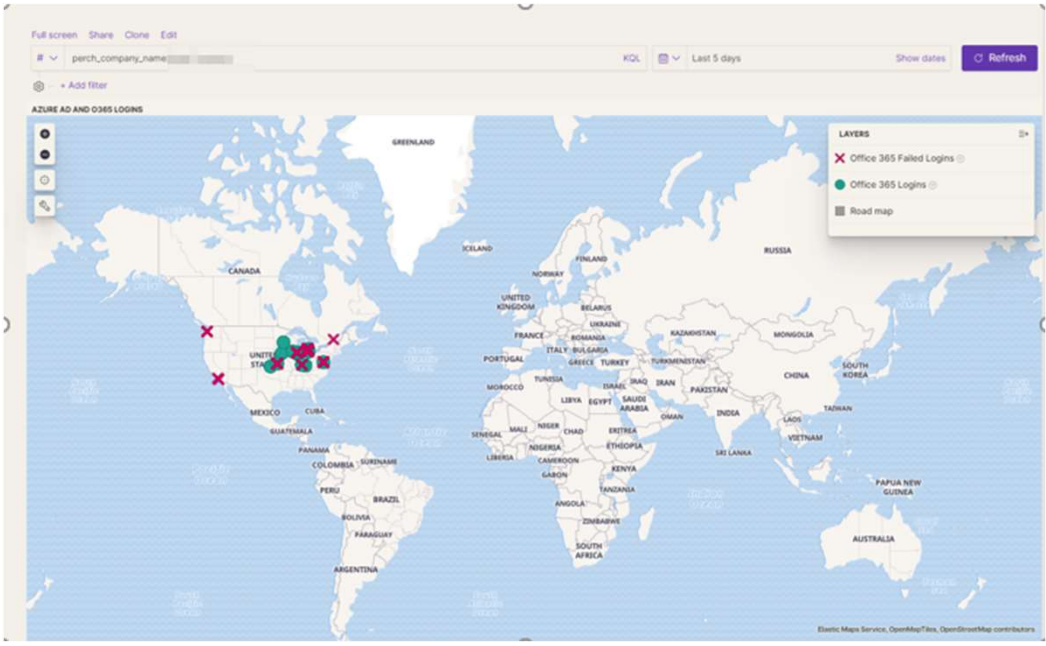
Why Security Controls Matter

During an incident with no security controls



Before
Is this you today?

Few days later with controls in place



After
Or is this you today?

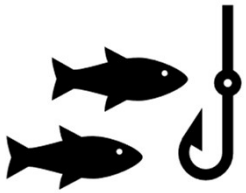
Rising cost of an incident…

Above costs are averaged for a 200-250 employee company in 2020

**** This is not representative of all costs.**

Incident Response Firm	$50-150K
Ransom	$175K (Often start much higher)
Incident Recovery Services	$200K+
Recovery Equipment	Varies - $25-300K not uncommon
Legal Services	$25K
Downtime	Cost per hour down varies Average to partial recovery is 72 hours, weeks for full recovery
Cost without Cyber Insurance	**$450K – $850K+**
Cost with Cyber Insurance	**Deductible plus overages or coverage gaps… NOT ZERO!**

Reality of Phishing



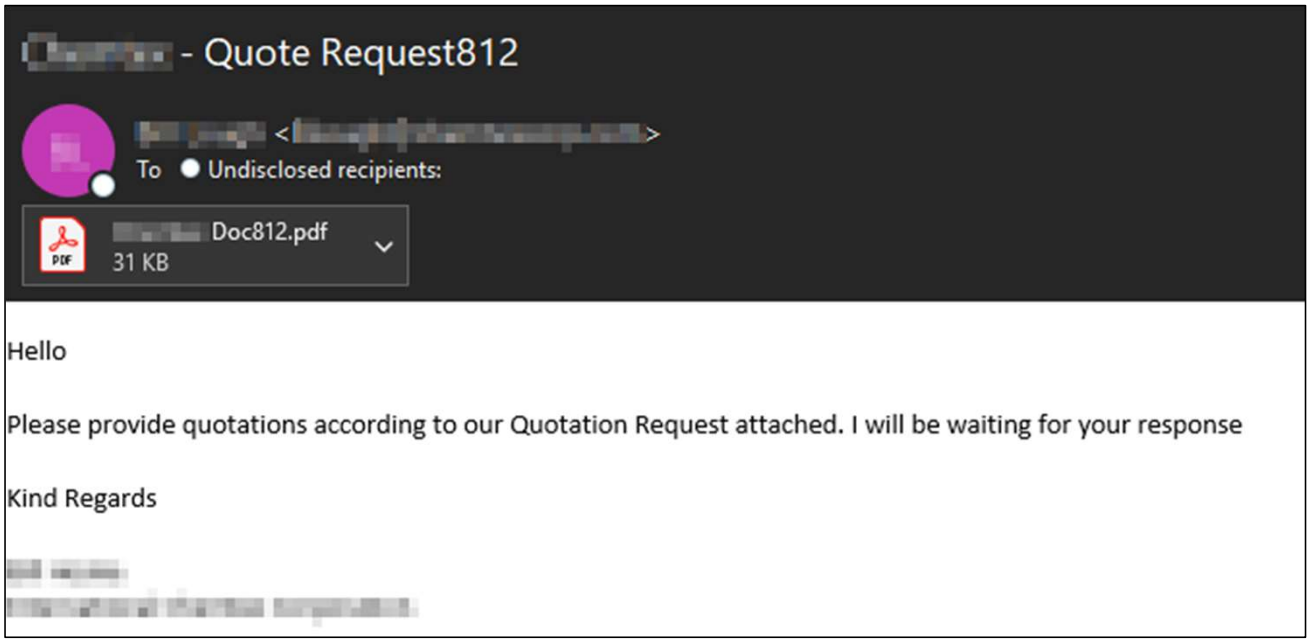
Phishing Leads to:

Business Email Compromise (BEC)
Corporate Account Takeover (CATO)

Consequences:

Circle of influence is at risk
Wire Fraud
Intellectual Property and Protected Information
Ransomware (Extortion and Exfiltration)
Reputation Damage
Required Reporting
Loss of Employment

Examples



Examples

Here's the document that [redacted] shared with you.

This link will work for anyone.

[redacted]

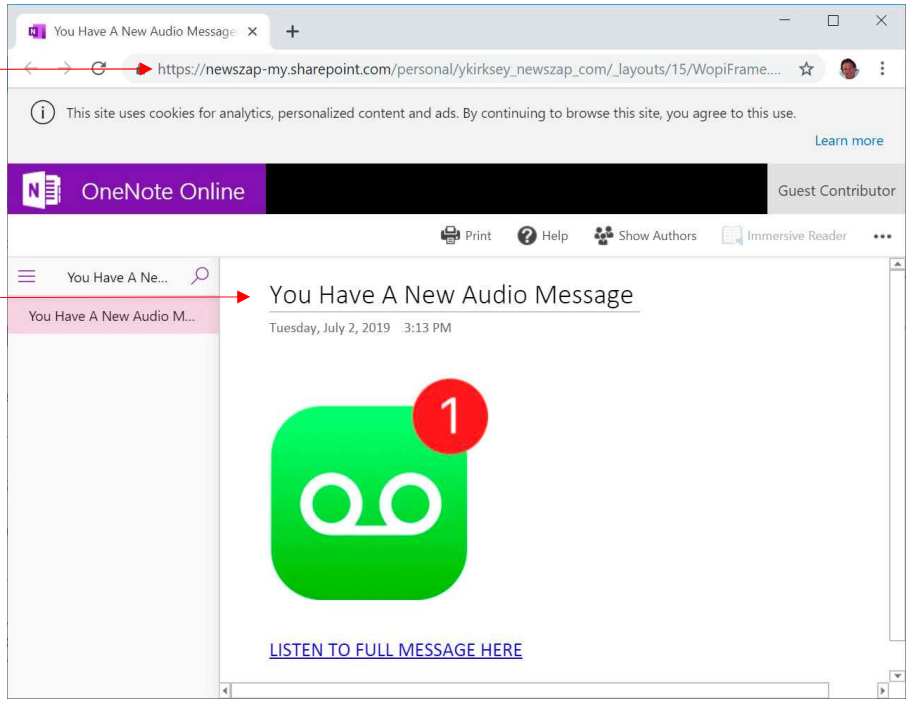
Open

Sender will be notified when you open this link for the first time.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

?

?



Bad guys use good things…

Reality of Ransomware

Ransomware Reality:

Ransomware is significantly on the rise again

Time is critical, but containment and forensics take time

Ransomware often exfiltrates data

Consequences:

Inability to operate

Loss of business

Significant financial impact (even with insurance)

Reputation damage

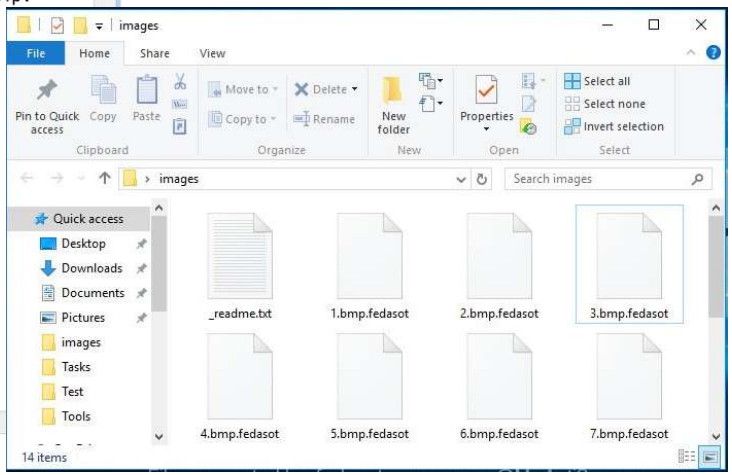
Bankruptcy

Examples

FA30D-Readme - Notepad

File Edit Format View Help

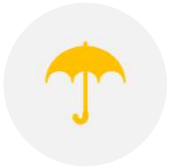
```
Hi!
Your files are encrypted.
All encrypted files for this computer has extension: .fa30d

--

If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compromised,
rebooting/shutdown will cause you to lose files without the possibility of recovery and even god will not be able to help you,
it could be files on the network belonging to other users, sure you want to take that responsibility?

--

Our encryption algorithms are very strong and your files are very well protected, you can't hope to recover them without our help.
The only way to get your files back is to cooperate with us and get the decrypter program.
Do not try to recover your files without a decrypt program, you may damage them and then they will be impossible to recover.

We advise you to contact us as soon as possible, otherwise there is a possibility that your files will never be returned.
For us this is just business and to prove to you our seriousness, we will decrypt you some files for free,
but we will not wait for your letter for a long time, mail can be abused, we are moving on, hurry up with the decision.

Contact us:
1.sevenoneone@cock.li
2.kavariusing@tutanota.com

Don't forget to include your code in the email:
{code_a35f346f_fa30d:
leZJOKucvM4/UMdFgSxtROL1+eLllWettSWxMsedwjT+LpOUMY
SXUmU7+RuA5KenynCDaGOTCsoqI8XNLaokSOcjk9BU7U8gbzRf
owsuCVKUvLdjh8r7JoOgROpk1Kc938cr7TjG7sBShNSg23jGeZ
At/CRkt36bozEfHiwdigTRUkY7caoZtyHKRzyQmFjeJF+Nc+EN
O7lkHY9D1gaP2JZIOXc67P0R3JCNTRIfICQpZrwf3JUuOtMHye
TziI9ygRg2a4ROy9UYitwiyS9UvDSwdFO=}
```



What to Expect

Fear, Uncertainty, Doubt – Panic!

Lack of preparedness – what are next steps?



Your Cyber Insurance will help you, correctly. Use them!

Containment and Recovery will not go as fast as you want.

Your response process and technologies may deviate from the plan.

Legal involvement. Use Breach Counsel provided by cyber insurance.

Your business will be different than pre-incident.

Overtime, lack of sleep, and burn out.

Know your terminology. Do not use the word “Breach”.

What do I do about it?

Assess – Know your risks, posture, and maturity level

Have a Plan (Incident Response, Business Continuity, DR, Insurance, Know who to call)

Test your plan – Tabletops, Walkthroughs, Simulations

Mature – Establish security targets and improvements as part of business plan

Repeat – Re-assess periodically as technology and risks change over time