lumifi

Cyberattacks, Ransomware, and Fraudsters, Oh My!

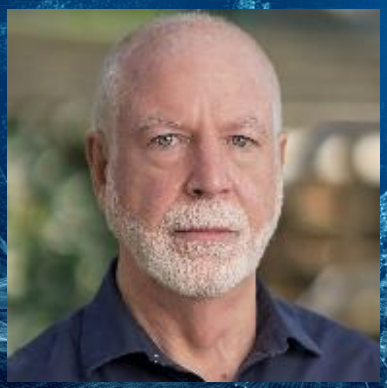
AWC
ASSOCIATION OF WASHINGTON CITIES

www.lumificyber.com

1

lumifi

Your Presenter



Mike Hamilton

***Field CISO**: Lumifi Cyber*
***Founder**, CISO: Critical Insight*
***Founder**: The PISCES Project*
***CISO**: City of Seattle*
***Policy Adviser**: WA State*
***Vice-Chair**: DHS Government Coordinating Council*
***Managing Consultant:** VeriSign Global Security*
***Ocean Scientist**: NASA/JPL*

2

lumifi

Why are you here?

- The services operated by your organization are critical: ***water purification, waste treatment***, ***emergency management, 9-1-1, elections***, and more
- Information technology holds all that up
- That technology is under attack, those services are at risk
- There's stuff you need to know

3

lumifi

What's the takeaway?

- There are a few ways that computers and networks are compromised, and steps you can take to prevent this
- You are constantly being hit with "bait", and it's coming from every communication medium
- Targeting and research are now part of the bad guy playbook

4

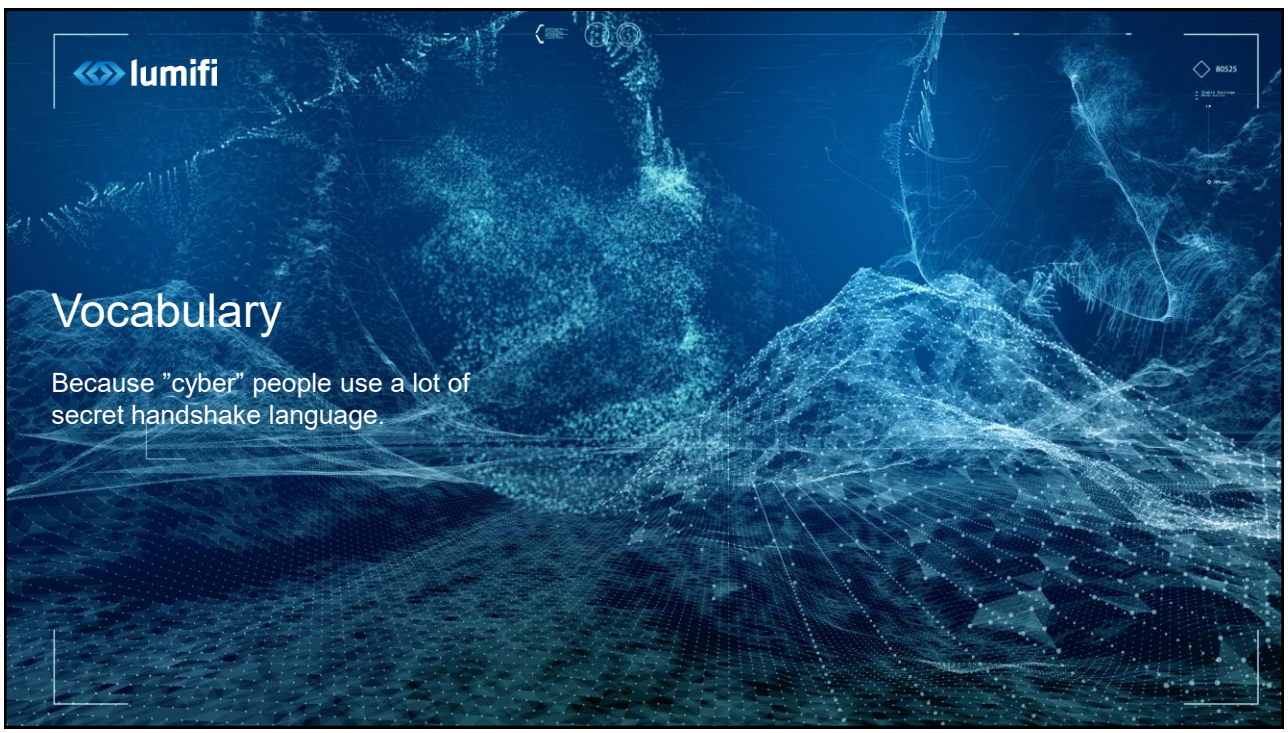
lumifi

5 Outcomes We Want To Avoid:

1. Unauthorized disclosure of protected records
2. Theft
3. Extortion
4. Your network used to attack others
5. Destructive disruption

Each can come with the additional impacts of civil litigation, claims of negligence, regulatory fines, and more.

5



6

lumifi

Ransomware – One form of extortion

Ransomware as a Service Threat Grows Against Local Governments

Cyberattack attempts on Nevada state websites increased 300% after August ransomware attack

Ransomware gang claims attack on St. Paul city government

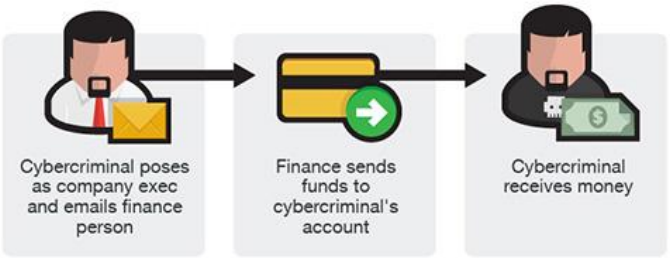
Ransomware Attack Targets Orleans Parish Sheriff's Office

7

lumifi

Business Email Compromise (BEC)

Carbon black supplier Orion loses $60 million in business email compromise scam



Low: I send you an invoice and your Accounts Payable pays it

Medium: The "Finance Director" asks you to buy gift cards or make an "emergency wire transfer"

High: An employee paycheck or vendor payment is redirected to a new bank

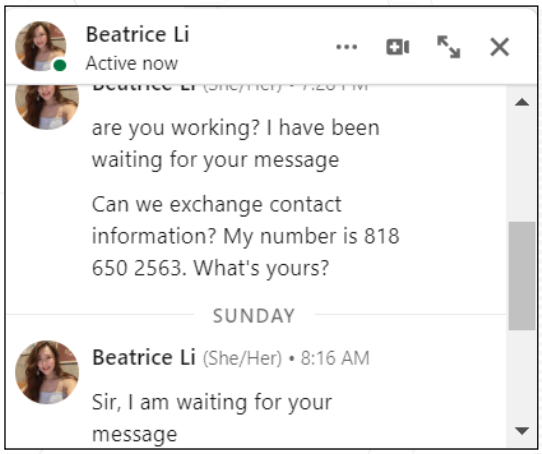
8

lumifi

Omaha City Councilwoman proposes crypto scam warning signs at kiosks

“Pig Butchering”

- Romance scam meets crypto
- Uses fake personas to gain trust
- Introduces an “investment opportunity”
- Fake portal shows gains that cannot be withdrawn
- Crypto wallet is drained
- Perps disappear

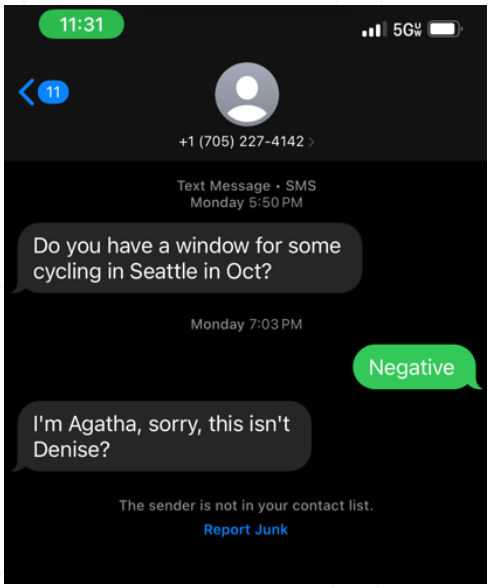


9

lumifi

Also Shows Up Like This

- A variety of reach-out tactics to start a conversation
- “I have your number in my call list but don’t know who you are”
- “Any luck on sending your best email so I can send you an application?”
- Do. Not. Engage.



10

11

lumifi

CREDENTIAL ABUSE

Low-End Methods

- ***If any of your passwords are on this list, your wounds are self-inflicted***
- Unchanged default passwords
- Phishing and vishing (we'll come back to this)
- Password guessing / Dictionary attack
- Dumps of stolen passwords - did you share?

1. password
2. 123456
3. 123456789
4. guest
5. qwerty
6. 12345678
7. 111111
8. 12345
9. col123456
10. 123123

www.lumificyber.com

12

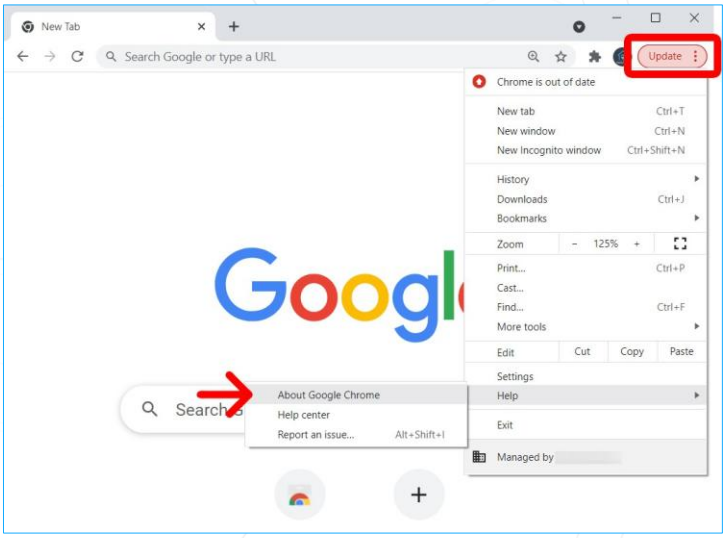
lumifi

CREDENTIAL ABUSE

Mid-Range Methods

- Credential stuffing
- Causing “MFA Fatigue”
- Infostealers

An unpatched browser + site rigged with an infostealer + bait to draw you to that site: **All your passwords now belong to the bad guy**



13

lumifi

CREDENTIAL ABUSE

Credential Stuffing

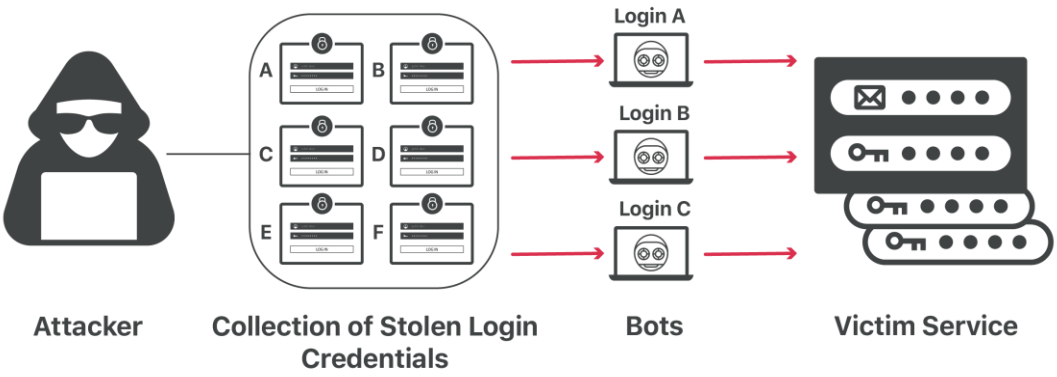
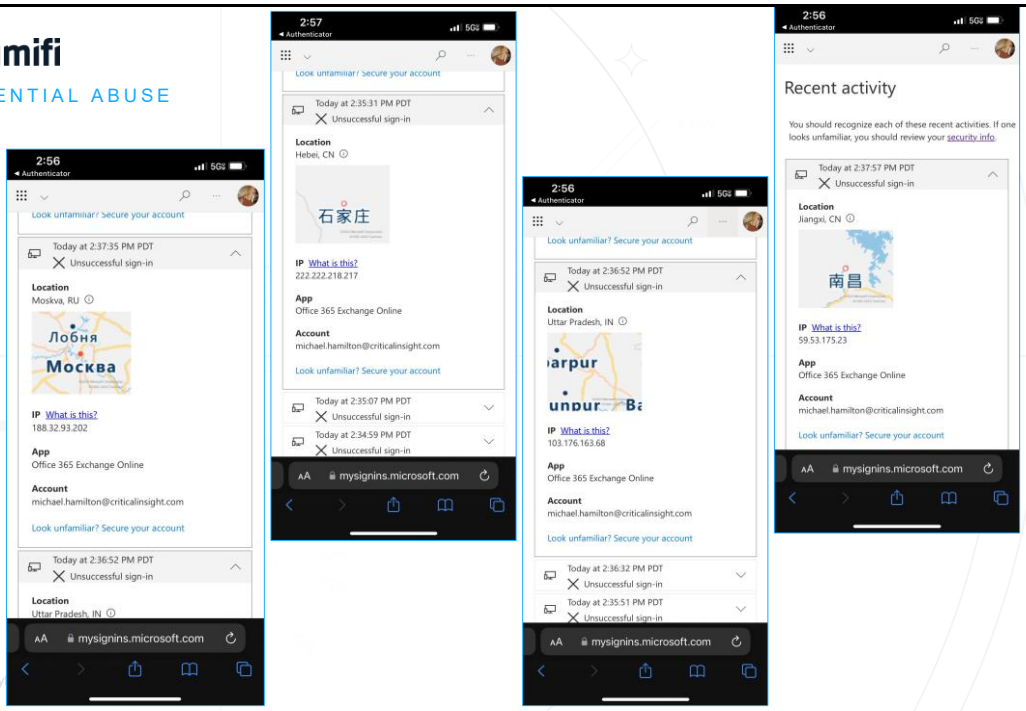


Image Credit: OWASP Foundation

14

lumifi

CREDENTIAL ABUSE



15

lumifi

CREDENTIAL ABUSE

High-End Methods

- SIM-swapping
- Active session token stripping and reuse
- ***Threats of violence*** to disclose a password

Problematically, we now have domestic threat actors that are fluent in English and telecommunication company processes.

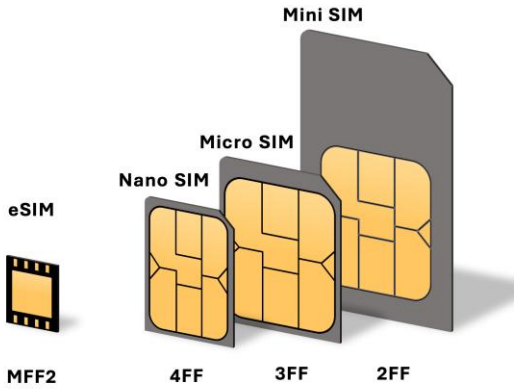


Image Credit: Wikipedia

16

lumifi

SPECIAL TOPIC

Session Token Stripping

1. Phishing link goes to a hosted script that grabs the session cookie
2. Connection to Microsoft proxied through bad guy system
3. Successful MFA challenge marked bad guy session as ‘MFA succeeded’
4. Bad guy now has access to O365, SharePoint, Teams, and likely all your SSO applications

It took less than one minute.

17

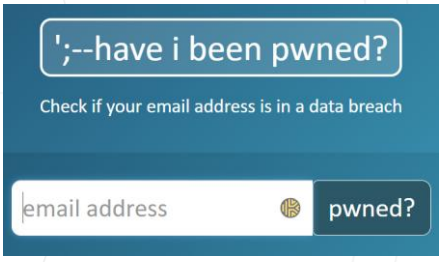
lumifi

SPECIAL TOPIC

Avoiding Credential Abuse

- Use pass phrases – first sentence of a book, or five words separated by spaces
- Combine with multi-factor authentication (we’ll come back to that)
- Use a password vault, and ***unique passwords*** with every system or service you access
- Do NOT store passwords in browsers
- Check your e-mail addresses on haveibeenpwned.com
- Do not click unexpected links you receive

NIST Drops Password Complexity, Mandatory Reset Rules



18

lumifi

Three Most Prevalent Tactics

#2 Vulnerability Exploit

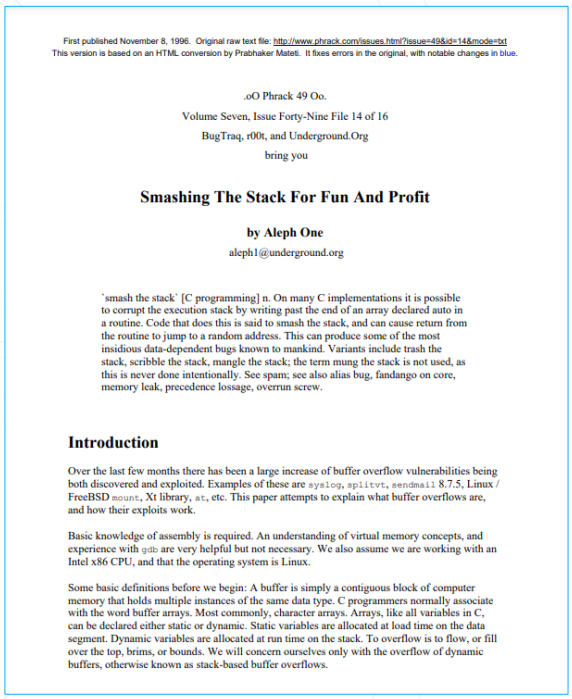
19

lumifi

VULNERABILITY EXPLOIT

What is a vulnerability?

Vulnerabilities can be problems in how the software was coded – for example allowing the memory space assigned to a variable in the software to be exceeded (known as a “buffer overflow”).



First published November 8, 1996. Original raw text file: http://www.phrack.com/issues.html?issue=49&id=14&mode=txt
This version is based on an HTML conversion by Prabhaker Mateti. It fixes errors in the original, with notable changes in blue.

.oO Phrack 49 Oo.

Volume Seven, Issue Forty-Nine File 14 of 16

BugTraq, r00t, and Underground.Org

bring you

Smashing The Stack For Fun And Profit

by Aleph One

aleph1@underground.org

`smash the stack` [C programming] n. On many C implementations it is possible to corrupt the execution stack by writing past the end of an array declared auto in a routine. Code that does this is said to smash the stack, and can cause return from the routine to jump to a random address. This can produce some of the most insidious data-dependent bugs known to mankind. Variants include trash the stack, scribble the stack, mangle the stack; the term mung the stack is not used, as this is never done intentionally. See spam; see also alias bug, fandango on core, memory leak, precedence lossage, overrun screw.

Introduction

Over the last few months there has been a large increase of buffer overflow vulnerabilities being both discovered and exploited. Examples of these are `syslog`, `splitvt`, `sendmail` 8.7.5, Linux / FreeBSD `mount`, Xt library, `at`, etc. This paper attempts to explain what buffer overflows are, and how their exploits work.

Basic knowledge of assembly is required. An understanding of virtual memory concepts, and experience with `gdb` are very helpful but not necessary. We also assume we are working with an Intel x86 CPU, and that the operating system is Linux.

Some basic definitions before we begin: A buffer is simply a contiguous block of computer memory that holds multiple instances of the same data type. C programmers normally associate with the word buffer arrays. Most commonly, character arrays. Arrays, like all variables in C, can be declared either static or dynamic. Static variables are allocated at load time on the data segment. Dynamic variables are allocated at run time on the stack. To overflow is to flow, or fill over the top, brims, or bounds. We will concern ourselves only with the overflow of dynamic buffers, otherwise known as stack-based buffer overflows.

www.lumificyber.com

20

lumifi

VULNERABILITY EXPLOIT

What *else* is a vulnerability?

- A vulnerability can also be a configuration problem, for example failing to change a default password that is widely known.
- A vulnerability can also be the result of human behavior, for example failing to train users on good security hygiene leaves them vulnerable to phishing attacks.

21

lumifi

VULNERABILITY EXPLOIT

Recent News

US and UK govts warn: Russia scanning for your unpatched vulnerabilities

Recent Splunk Enterprise Vulnerability Easy to Exploit: Security Firm

Ransomware attackers exploit year-old backup vulnerability

Telegram zero-day for Android allowed malicious files to masquerade as videos

The Potential Impact of the OpenSSH Vulnerabilities CVE-2024-6387 and CVE-2024-6409

22

lumifi

VULNERABILITY EXPLOIT

It's now a race!

- When a patch is released and a vulnerability made public:
- Criminals and nation-states go to work immediately
- The patch is reverse-engineered to find out what it "fixes"
- The Internet is scanned for vulnerable targets
- Exploit is automated

159 CVEs Exploited in Q1 2025 — 28.3% Within 24 Hours of Disclosure

91% of Cyberattacks Targeted Multiple Organizations Using Mass Scanning to Uncover and Exploit Vulnerabilities

Hackers scan for vulnerabilities within 15 minutes of disclosure

23

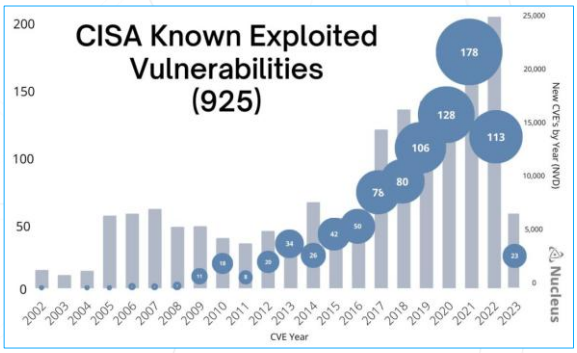
lumifi

VULNERABILITY EXPLOIT

Avoiding Vulnerability Exploit

- Keep on top of vendor announcements
- Score your vulnerabilities (ask me for policy)
- Use the known exploited vulnerabilities catalog
- If it's critical for an asset accessible from the Internet:

DROP WHAT YOU ARE DOING AND APPLY THE PATCH



CVSS
COMMON VULNERABILITY SCORING SYSTEM

24

25

lumifi

SOCIAL ENGINEERING

Cognitive biases that aid social engineers

- ***Halo Effect*** – a positive view of a company being spoofed
- ***Hyperbolic Discounting*** – e.g., "free trial"
- ***Curiosity Effect*** – news headlines and current events
- ***Authority Bias*** – unconsciously influenced by someone with authority (the "CEO")
- ***Confirmation Bias*** – being presented with something you agree with

Over 75% of cyber-attacks are caused by human failures, while less than 25% are because of technology miscues.

Over 90% of cyberattacks begin with a phishing email.

www.lumificyber.com

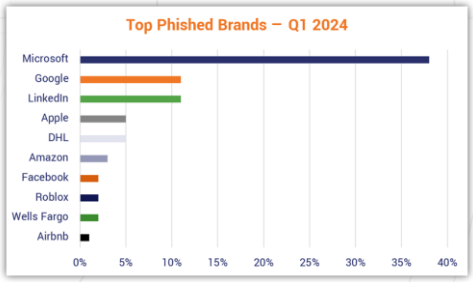
26

lumifi

SOCIAL ENGINEERING

Phishing

- Fake lookalike sites that simulate known brands and products: Sharepoint, Microsoft, DocuSign, DropBox, Adobe, many others
- Get you to give up credentials, follow a link, download a file, etc.
- Easy-to-use kits



Images Credit: The SSL Store

27

lumifi

SOCIAL ENGINEERING

Smishing – Fake Failed Delivery

- Phishing over SMS (text)
- Not expected
- Doesn't include tracking information
- The instructions are strange
- VirusTotal says malicious/phishing
- Could compromise your phone

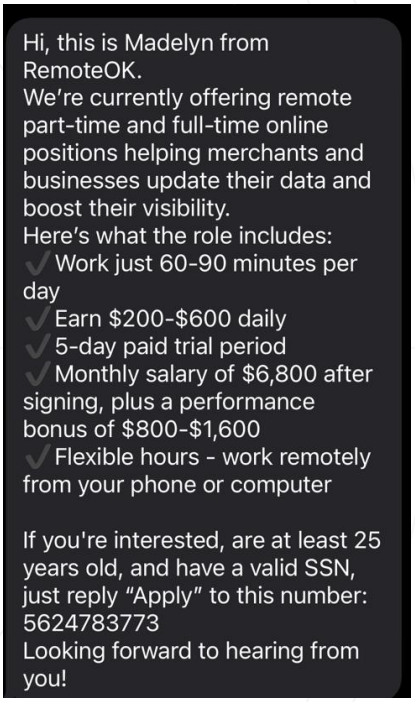
28

lumifi

SOCIAL ENGINEERING

Smishing – Fake Job Offer

- Will ask for a lot of personal information
- Wants your bank account for direct deposit
- Will guide you through 2 small deposits
- Will drain your bank account



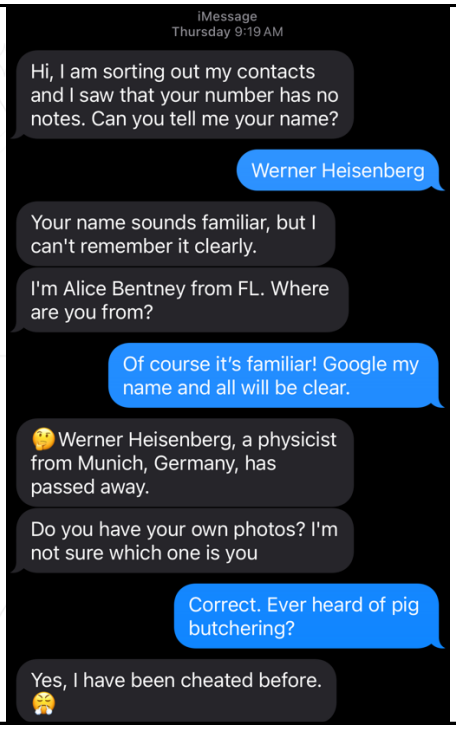
29

lumifi

SOCIAL ENGINEERING

Pig Butchering by SMS

- Wants personal relationship
- Will introduce "investment"
- You invest a little – portal shows money growing
- You invest more to gain more
- "Alice" disappears with your money



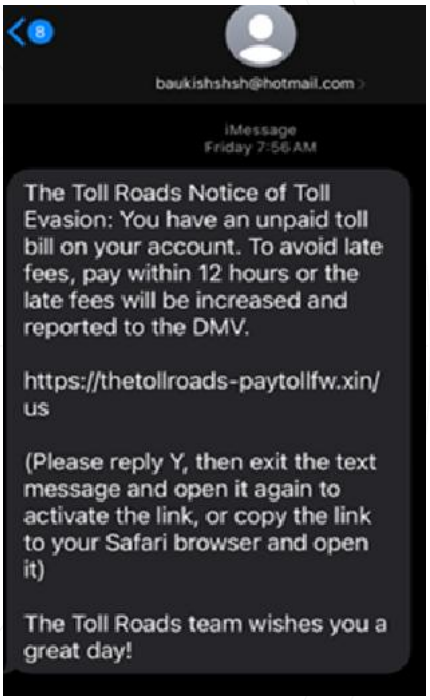
30

lumifi

SOCIAL ENGINEERING

Current Fraud Campaign

- Notice of “Toll Evasion”
- Comes from a Hotmail address
- Wants a response before activating the link
- Will ask for credit card or other payment method



31

lumifi

SOCIAL ENGINEERING

Vishing – Voice Phishing

- Taking a caller’s word at face value can result in compromise
- Verify the identity of the caller as independently as possible
- Do not type a URL someone gives you over the phone
- Grandchild in trouble – classic scam
- Now using **deepfakes** to simulate voice

AI Voice Doppelgänger: Hackers Impersonate White House Chief of Staff After Phone Breach; Urgent Probe Underway

Hacker Poses As Support Rep To Breach Cox Communications

‘Mom, these bad men have me’: She believes scammers cloned her daughter’s voice in a fake kidnapping

Dubai: Billionaire nearly lost huge amount of money after staff gets call from 'AI clone'

32

lumifi

SOCIAL ENGINEERING

Deepfakes

- Remarkably easy to produce
- Already used in political ads
- Watch out for fake job applicants using deepfake audio and video interviews

Scammers siphon $25M from engineering firm Arup via AI deepfake 'CFO'

Deepfake Putin warning Americans about their impending doom

lumifi

SOCIAL ENGINEERING

Deepfakes

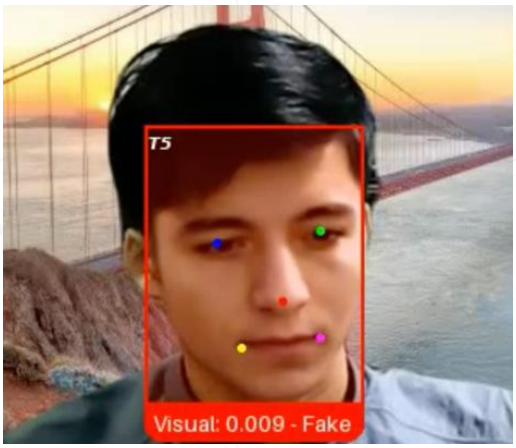
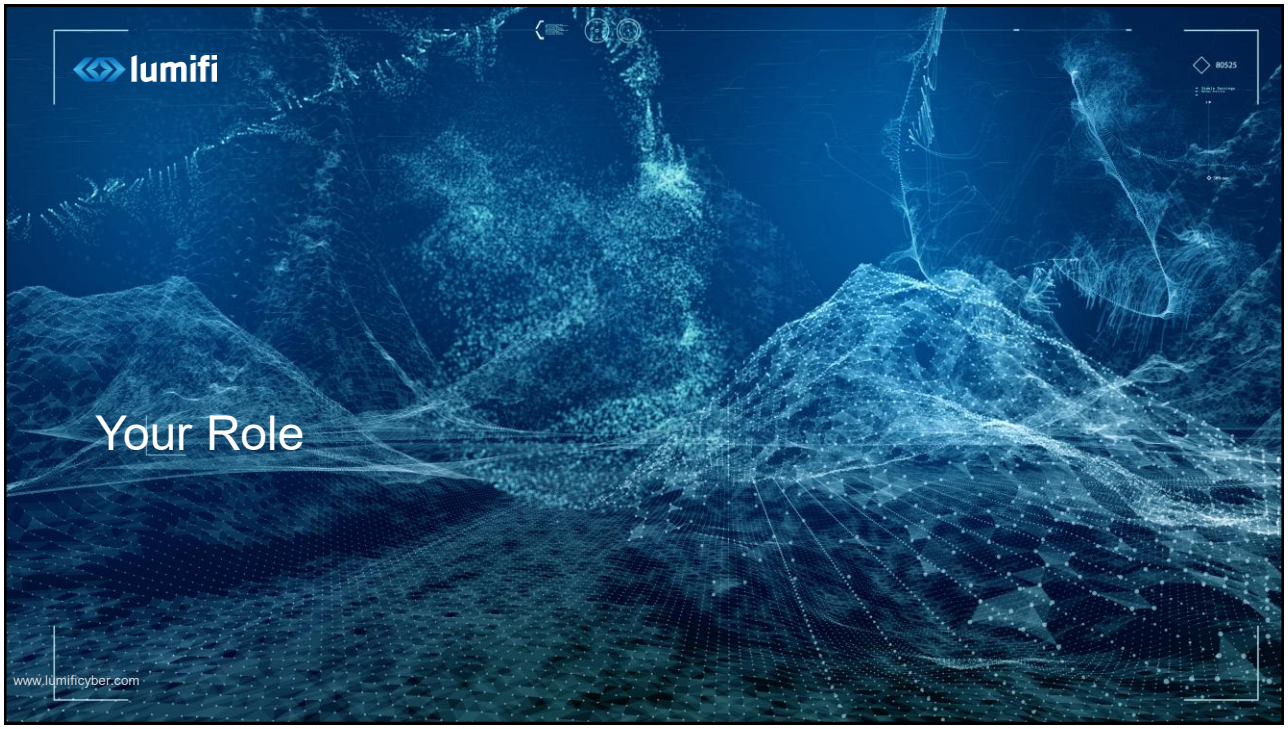


Image credit: CBS News

- Fake job applicants
- Executive/Elected impersonation
- Employee impersonation for password reset
- Help desk impersonation



35

lumifi

Information Security Program Management			
Weekly	**Monthly**	**Quarterly**	**Annually**
Weekly Report	Conduct vulnerability Assessment	Access authorization management reviews	Penetration test
Incident Management	Review vulnerability assessment results, assign disposition and delegate	Conduct Risk Governance Committee meeting	Risk Assessment
Recordkeeping (e.g. security testing results for products)	Firewall rules review	Perform 2 of the annual requirements	Security Awareness Training / Attestation
Corrective action board; infosec ritual			Tabletop or functional security exercise
Meetings (change control, infosec, governance, etc.)			Policy review
Consulting project management			Service audits
Ad-hoc service requests (access changes, e.g.)			Participate in annual planning and budget development
Planning for upcoming monthly, quarterly, or annual requirements			Vendor risk assessment

- **This is what acybersecurity program looks like**
- **A full program is beyond the capabilities of small local governments**
- **Focus on credential management, user training, and rapid patching of vulnerabilities**
- **Use grant funding for assessments, capital purchases**
- **Participate in risk governance**

36

lumifi

Risk Governance

- CALLED OUT IN V2.0 OF THE NIST CSF
- SEC, HHS, OTHER SRMAS ALL WANT RISK GOVERNANCE
- THIS MEANS PUTTING ***EXECUTIVE FINGERPRINTS ON RISK DISPOSITIONS***
- MUST DOCUMENT YOUR RISK THRESHOLD TO JUSTIFY ACCEPTED RISKS
- YOU MUST HAVE AN EXCEPTION PROCESS

Cybersecurity Practice #10 has been updated from Cybersecurity Policies to Cybersecurity Oversight and Governance

In addition to policies, this section includes governance and oversight structures each organization should have in place for an effective cybersecurity program.

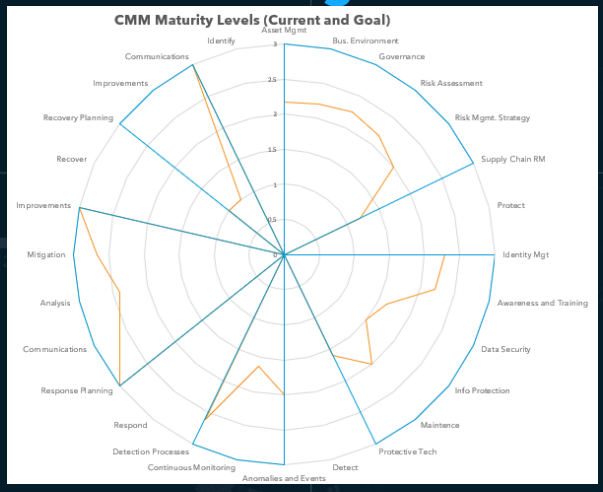
Health Industry Cybersecurity Practices

37

37

lumifi

On Measuring Risk



www.lumificyber.com

Qualitative or Quantitative?

What is the framework used?

Aligned with a maturity model?

Can risk be expressed in dollar estimates for unwanted business disruptions/outcomes?

Annualized Loss Expectancy for:

- Records disclosure
- Theft
- Extortion
- Disruption
- Being used to attack others

38

lumifi

What's The Value of Risk Governance?

- Reasoned resourcing of risk mitigation treatments
- Can provide safe harbor from civil litigation and claims of negligence

PowerSchool data breach brings claims of negligence, poor cyberhygiene

Paychex sued for negligence after data breach exposes workers' names and Social Security numbers

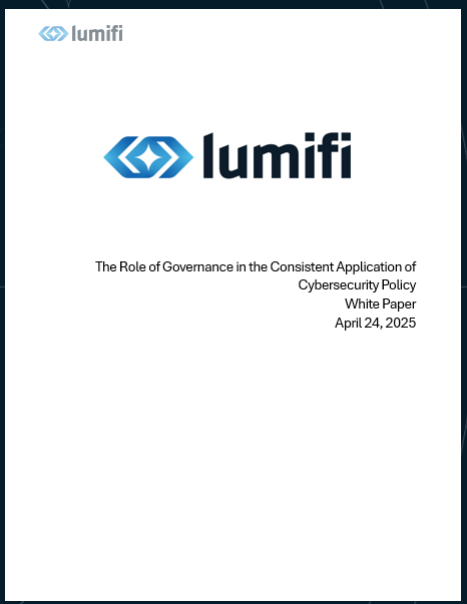
H&R Block class action alleges negligence in data breach

39

lumifi

You Can Have This.

- White paper on drivers and benefits of risk governance
- Written at the request of a large County government
- Meant to address a lack of accountability in aligning agencies with policy
- Brings stakeholders to the table and creates records of decisions

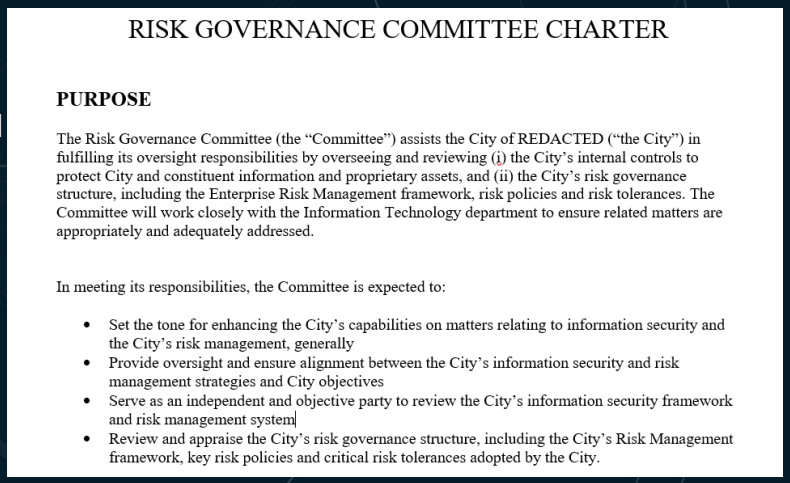


40

lumifi

You Can Have This.

- Risk Governance Committee Charter
- Modified for use in local government and state agencies
- Includes executive membership representing Finance
- Elected Officials are encouraged as members



RISK GOVERNANCE COMMITTEE CHARTER

PURPOSE

The Risk Governance Committee (the "Committee") assists the City of REDACTED ("the City") in fulfilling its oversight responsibilities by overseeing and reviewing (i) the City's internal controls to protect City and constituent information and proprietary assets, and (ii) the City's risk governance structure, including the Enterprise Risk Management framework, risk policies and risk tolerances. The Committee will work closely with the Information Technology department to ensure related matters are appropriately and adequately addressed.

In meeting its responsibilities, the Committee is expected to:

- Set the tone for enhancing the City's capabilities on matters relating to information security and the City's risk management, generally
- Provide oversight and ensure alignment between the City's information security and risk management strategies and City objectives
- Serve as an independent and objective party to review the City's information security framework and risk management system
- Review and appraise the City's risk governance structure, including the City's Risk Management framework, key risk policies and critical risk tolerances adopted by the City.

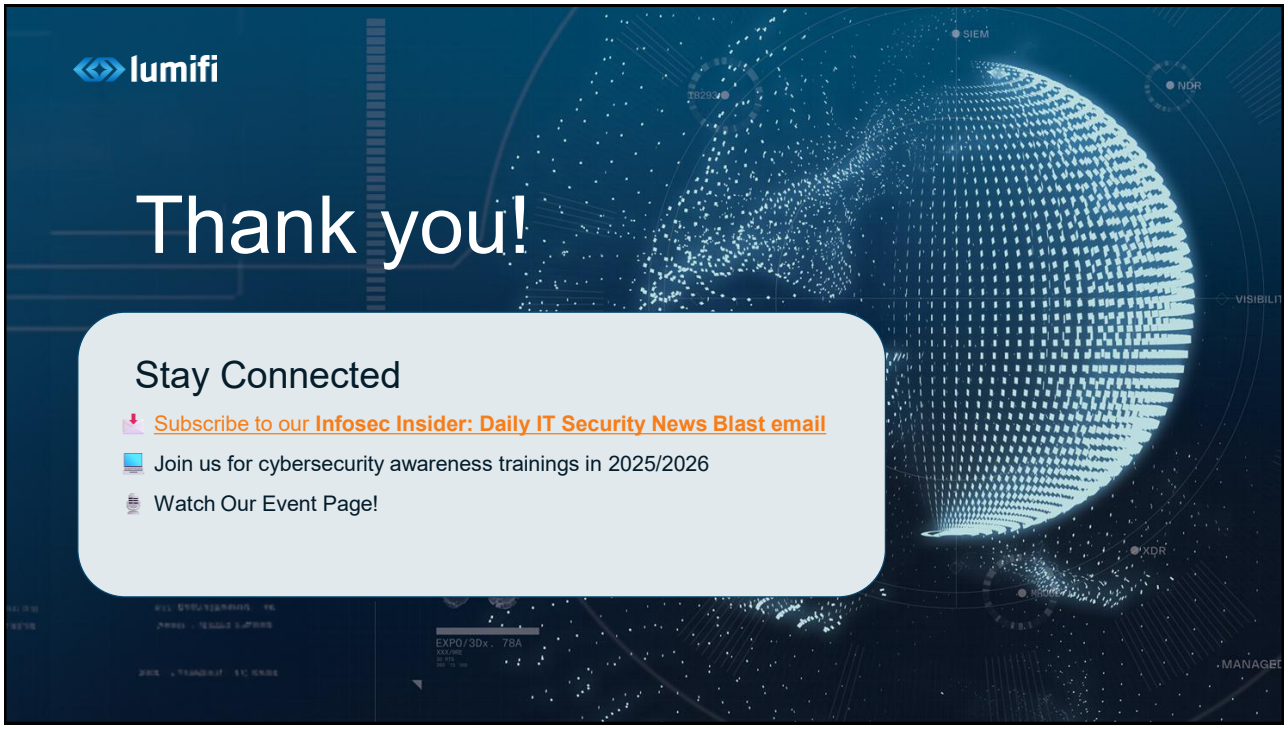
41

lumifi

Lastly…

Rescinding the policy of de minimus use of government technology will reduce your "attack surface" by 40%

42


lumifi
Thank you!
Stay Connected
Subscribe to our Infosec Insider: Daily IT Security News Blast email
Join us for cybersecurity awareness trainings in 2025/2026
Watch Our Event Page!
SIEM
NDR
XDR
MANAGED

43