

Cyber

De-Constructed

Presented By:

Darren J Faye, BSIT, CCIC, CyRM, CIC, CWCC, CRIS
AssuredPartners

October 18, 2023

Objectives

- Explain what cyber exposures are
- Measure the cost of breaches and what's at stake
- Identify areas where exposure can be controlled
- What to do before a breach
- Transferring the exposure somewhere else
- What is happening during a breach
- What do you do following a breach
- Self-assessment

Part I

- What is cyber?
 - Dictionary
 - Relating to or characteristic of the culture of computers, information technology, and virtual reality. The “cyber age”.

What is “cyber” really?



1 day ago

September revenue at MGM Springfield casino incomplete following data breach

masslive.com - Jim Kinney



2 days ago

How hackers piled onto the Israeli-Hamas conflict

politico.eu - Antoaneta Roussi, Maggie Miller

Lower-level cyberattacks are becoming a major



10 hours ago

Bank account numbers & PINs leaked in cybersecurity attack at Charlotte-based AvidXchange

wsocvtv.com - Cassia Sari



AssuredPartners

What Big Tech knows about you RIGHT NOW!

- Personal Info – Name, Birthday, Gender
- Location/Address/Usual Routes – phone tracking
- Relationship Status
- Work Status/Income Level
- Educational Background
- Ethnicity
- Religious/Political Beliefs
- Facial Data Recognition
- Financial/Banking Info
- IP Address
- Communications (past calls)
- Calendar Events
- Search History
- Audio Recordings (Alexa, Google Home, Siri)
- Media Consumed
- Web-Browsing History (sites you go to)
- Social Media Behavior
- Purchase History
- Fitness/Health Data
- Clicked Ads
- Posts Hidden from Facebook News Feed
- Devices Used

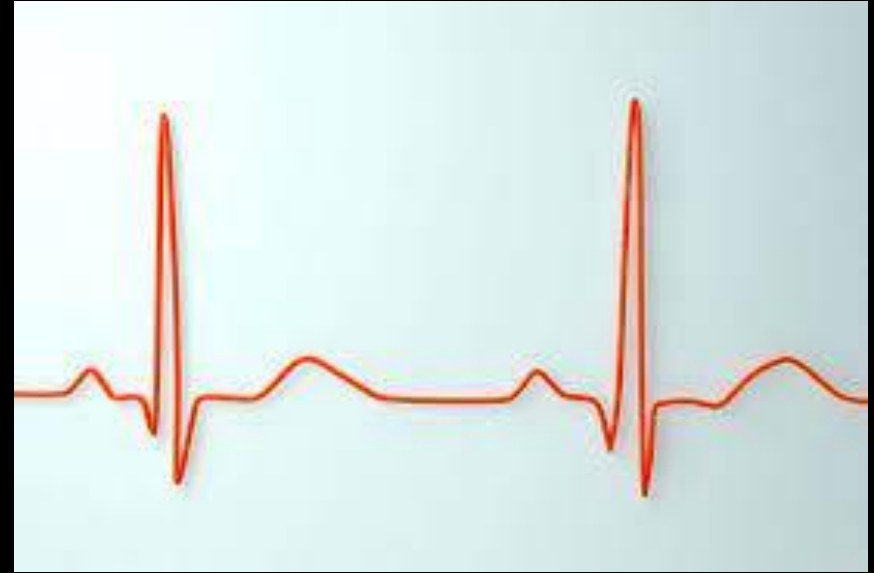


...and why should I care?

- SSN (\$4)
- Banking Systems (\$120)
- Credit Cards (\$240)
- Health Systems (\$250)
- Computers (\$600/10k)
- Social Media (\$80)
- Cell Phones/SIM Swapping (\$200)

Or they can use stolen info for:

- Doxing
- Impersonating and Defrauding



What many don't know...

F 52	APPLICATION SECURITY	15 ISSUES
B 80	CUBIT SCORE	2 ISSUES
A 90	DNS HEALTH	1 ISSUE
F 59	ENDPOINT SECURITY	3 ISSUES

D 69	IP REPUTATION	6 ISSUES
A 100	INFORMATION LEAK	0 ISSUES
D 67	NETWORK SECURITY	29 ISSUES
D 67	PATCHING CADENCE	9 ISSUES
A 100	SOCIAL ENGINEERING	1 ISSUE

!!! HIGH SEVERITY

SSL/TLS Service Supports Weak Protocol 25

!! MEDIUM SEVERITY

SSH Supports Weak MAC 7
 Certificate Is Expired 26
 Certificate Is Self-Signed 90
 TLS Service Supports Weak Cipher Suite 46
 RDP Service Observed 2
 PPTP Service Accessible 11
 rsync Service Observed 2
 Certificate Signed With Weak Algorithm 9
 SSH Supports Weak Cipher 6
 LDAP Server Accessible 3
 Remote Access Service Observed 3
 SMB Service Observed 4

! LOW SEVERITY

Telnet Service Observed 2
 Certificate Lifetime Is Longer Than Best Practices 30
 IP Camera Accessible 9
 Certificate Without Revocation Control 105
 FTP Service Observed 6

✓ POSITIVE

There are no Positive Signals for Network Security

i INFORMATIONAL

Networking Service Observed 345
 OpenVPN Device Accessible 4
 Oracle Service Registry Detected 1
 Website Uses GoDaddy TLS Certificates 1
 HTTP Proxy Service Detected 5
 UPnP Accessible 1
 Telephony/VoIP Device Accessible 3
 Mobile Printing Service Detected 1
 DNS Server Accessible 1
 Printer Detected 1
 Minecraft Server Accessible 1

The Internet of Things (IoT)

- Appliances
 - “Smart” anything
 - Wearables
 - Routers
 - Biometric Scanners
 - Cars
 - Crawlers/Dozers
-
- Low security, weak passcodes, insecure interfaces

Signals are Everywhere

- 31: Beacon
- 30: Beacon
- 29: Beacon
- 28: Beacon
- 27: Venus_AC0BFB13D542: Nestlé Nespresso
- 25: iPhone XR
- 24: Beacon
- 23: Windows 10 2018
- 22: Windows 10 2018
- 21: Apple Pencil [Paired]
- 20: Windows 10 2018
- 19: iPhone (2): iPhone 12 Pro Max
- 18: Beacon
- 17: Windows 10 2018
- 16: Logitech [Requested]
- 15: iPhone 13
- 14: Windows 10 2018

The image displays several screenshots from network analysis tools, likely Wireshark, illustrating various network protocols and sessions. The top-left screenshot shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Length. Packet 8 is highlighted, showing an HTTP GET request to http://server/.

The top-right screenshot shows the details pane for an LDAP bindRequest. It includes fields for name (ad\lpsadmin) and simple (password), both highlighted with red boxes.

The middle-left screenshot shows the details pane for an HTTP 400 Bad Request response. The Authorization header is highlighted with a red box, showing Basic authentication credentials.

The middle-right screenshot shows the details pane for an HTTP 400 Bad Request response. The body is highlighted with a red box, showing a JSON object with fields for username and password.


The bottom-left screenshot shows the details pane for an HTTP 400 Bad Request response. The body is highlighted with a red box, showing a JSON object with fields for email and password.

The bottom-right screenshot shows the details pane for an HTTP 400 Bad Request response. The body is highlighted with a red box, showing a JSON object with fields for email and password.

Cyber Claim Example #1

- I didn't send that invoice!

2. A Catchy Logo



Invoice

Invoice no.: 011
Invoice date: Jul 13th, 2022
Due: Jul 13th, 2023

6. The Invoice Number

From Saldo Apps
John Smith
wiz@saldoapps.com
80296979597
saldoapps.com
First str.28-32, Chicago, USA

3. Client Name and Contact Details

Bill to Shepard corp.
shepard@mail.com
80296979597
North str. 32, Chicago, USA

5. The Set Deadline

Ship to
North str. 32, Chicago, USA
Track #: RO80296979597

4. The Information About Your Goods or Services

DESCRIPTION	RATE, CADA	QTY	TAX	DISC	AMOUNT, CADA
Prototype Prototype-based programming is a style of object-oriented programming	20,230,450.00	2000	20.50%	20.50%	20,230,450.00
Design	20,230,450.00	2000	20.50%	20.50%	20,230,450.00

1. Payment Terms

Payment instruction
Paypal email
wiz@saldoapps.com
Make checks payable to
John Smith
Bank Transfer
Routing (ABA): 061120084

Subtotal: USD 8000.00
Discount (20%): USD 0.00
Shipping Cost: USD 0.00
Sales Tax: USD 450.00
Total: USD 8,480.00
Amount paid: USD 0.00
Balance Due: USD 8,480.00

7. "Thank You" Note

Notes
Prototype-based programming is a style of object-oriented programming in which behaviour

abe

In the news...

- 2,116 YTD publicly disclosed breaches (2022-1,862)
- 233M people affected (2022-425M)
- 3.8B records breached
- 4% of breaches were due to misconfigured databases
- Majority of breaches were due to:
 - Human error
 - Incorrect disclosure
 - Posting to wrong recipient

- Articles taken from SecurityMagazine.com



63% of organizations restore data after a ransomware attack

Security Staff

October 17, 2023

According to a recent data recovery report, 63% of organizations successfully restore their data when they experience a ransomware attack.



First half of 2023 sees more ransomware victims than all of 2022

Security Staff

October 11, 2023

A recent Deep Instinct report found that more victims were affected by ransomware in the first half of 2023 than in the entirety of 2022.

Top Data Breaches - 2023

Breach	When	# Affected
23andMe	Oct-23	TBD
Duolingo	Aug-23	3M
Maximus	Jul-23	11M
MOVEit	Jun-23	18M
ChatGPT	Mar-23	UNK
Lastpass	Mar-23	30M
T-Mobile	Jan-23	37M
Deezer	Jan-23	230M

Where do breaches come from?

- Physical Actions (11%)
- Privilege Misuse (12%)
- Social Engineering (17%)
- Human Error (17%)
- Malware (30%)
- Criminal Hacking (48%)

Cyber Claim Example #2

- I backed up, I restored, but I still lost...



Exposures

- Paper Files
 - Employee files
 - Client files
 - Payment/Bank/Credit Card statements and receipts
- Digital Files
 - Same as paper files, plus:
 - Intellectual Property
 - Copyrights
- The Network
 - Computers
 - Servers
 - Cloud
 - Everything in between



What's the big deal?

- Most people only use the Surface Web
 - Google
 - News Sites
- Some use the Deep Web
 - Academia
 - Medical Records
 - Intranets
- Very few even know about the Dark Web
 - Think “Mr. Robot”
 - Illegal sales of drugs and guns
 - TOR (the Onion Router)-encrypted sites

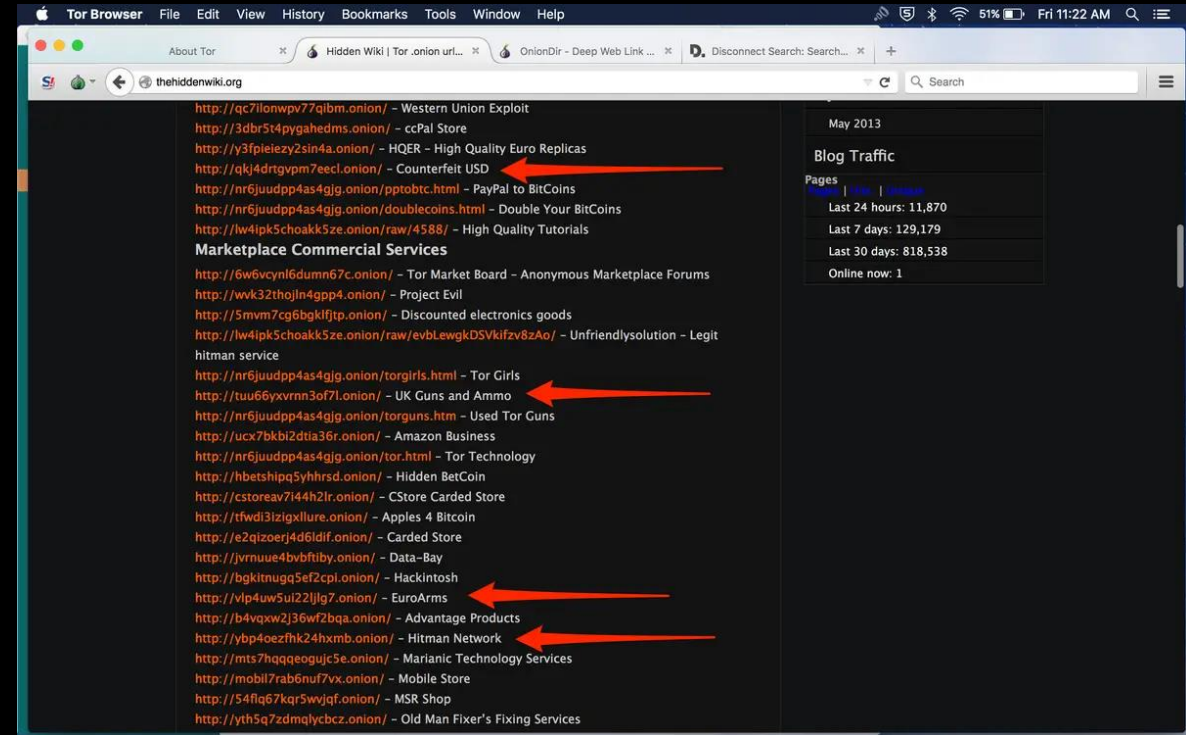


Image Credit: businessinsider.com

The Web

The web we use
vs. the Dark Web



Cyber Claim Example #3

Phishing for money



Part II – What's at stake?

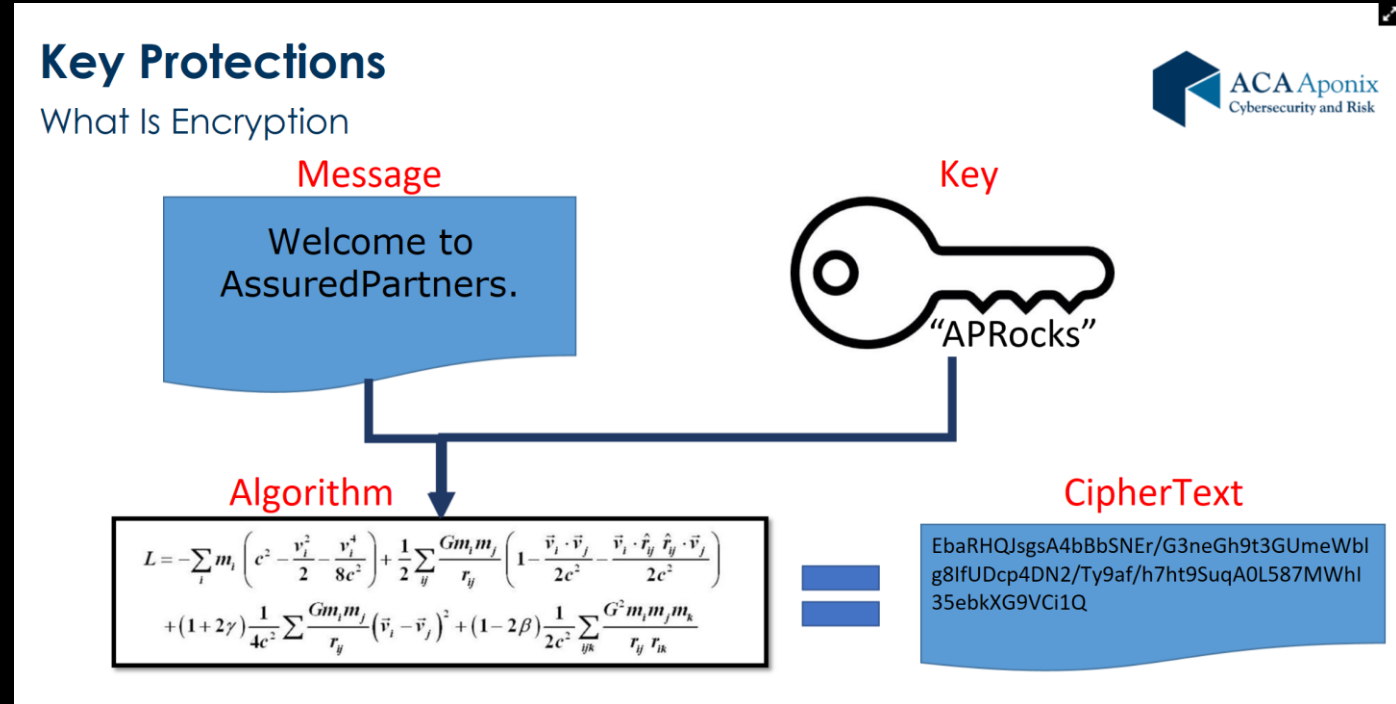


Direct and Indirect Costs of a Breach

- Average Cost of a Data Breach?
 - A modest 5,000 record breach of employee health information
 - \$343/record = \$1,713,875
 - 10,000 transactions involving customer payments
 - \$22/record = \$219,950
 - 15,000 records stolen from a customer database
 - \$148/record = \$2,220,000
 - Extortion Demands
 - \$300 (personal) to multi-millions
- Breach Fallout Costs
 - Reputational Damage
 - Lawsuits
 - Regulatory (Fed vs. State)

Before the Breach

- Change your passwords
 - Most common passwords (instantly cracked)
 - 123456
 - Password
 - 123456789
 - Qwerty
 - 1q2w3e
 - <https://howsecureismypassword.net>
 - <https://haveibeenpwned.com/>
 - Autumn = Instantly Cracked
 - Autumn23 = 2 hours to crack
 - Autumn23% = 4 weeks to crack
 - Autumn23%COLD = 3M years
 - my-wife-rules-the-house = 9 quintillion yrs
- Don't use the same passwords across sites
- Be wary of links in emails (do the hover)
- Use encryption and 2FA wherever possible
- Due to its low (but rising) cost, consider transfer to an insurance company (business & personal)



What does Cyber Insurance cover?

- First-Party Coverage*
 - Network security breaches
 - Cyber Extortion
 - Business Interruption
 - Transmission of virus or malicious code
 - Theft/destruction of data
 - Data exposed by hacker, lost device, rogue employee
 - Crypto-jacking

IMPORTANT: Prior acts coverage (must be endorsed)

*Subject to the actual terms of the policy. Not all policies include all coverage. Please read the forms carefully or ask your agent to verify coverage.

What does Cyber Insurance cover?

- Third-Party Coverage*
 - Network security breaches
 - Cyber Extortion
 - Transmission of virus or malicious code
 - Theft/destruction of data
 - Data exposed by hacker, lost device, rogue employee
 - Negligence in the performance of your services (E&O)
 - Infringement of Intellectual Property
 - Personal and Advertising Injury

*Subject to the actual terms of the policy. Not all policies include all coverage. Please read the forms carefully or ask your agent to verify coverage.

What does Cyber Insurance cover?

- Other Coverage usually included*
 - Forensic investigation
 - Legal advice
 - Notification costs and credit monitoring
 - Regulatory obligations/fines (including PCI)
 - Public relations expense
 - Loss of profit/extra expense
 - Dependent network business income
 - Social Engineering (make sure there is no call-back provision)
 - Cyber-Terrorism/War

*Subject to the actual terms of the policy. Not all policies include all coverage. Please read the forms carefully or ask your agent to verify coverage.

Cyber Claim Example #4

- IOT – uh oh!



AssuredPartners

What happens to my information during breach?

- Inventory what they just stole
 - Look through the data they just took for names, addresses, etc.
- Sell personal information
 - Likely to spammers and those sending phishing emails
 - Credit Card numbers might fetch \$0.25-\$250 (SSN = \$0.10-\$4)
 - Health Records can go as high as \$1,000
- Look for the Good Stuff (since people reuse passwords)
 - Government or military info (Passports up to \$2,000)
 - Large Corporations
 - LinkedIn Data (taken from the Dropbox hack)
- Offload the credit cards
 - Buy small gifts on Amazon to test them, then sell them
 - They lose value quickly
- Sell the balance in bulk after several months since it's about worthless

After the Breach

- Enlist the help of a (law)firm to help repair/minimize reputational damage (privilege)
- Follow the same steps before the breach
- Regularly go through a risk assessment to make sure you are aware
- Communicate with your employees the risks and steps to take (probably the single best thing to do)



Risk Management Must Haves/Considerations

- Do you have an incident response plan ready to go when needed?
- Do you offer training for your employees to help them identify scams?
- Does your organization rely on vendors for core business services?
- Do you have a password policy requiring strong passwords to access the system?
- Do you encrypt your data on computers and mobile devices?
- Do you use multi-factor authentication for your email or system access?
- What is your patching cadence (how often do you update your computers)?
- Do you use any endpoint detection/response system (ETDR)?
- Does your organization carry cyber insurance coverage?





Connect

Darren Faye

P/F/M/T: (330) 266-1914

darren.faye@assuredpartners.com



AssuredPartners