



Top Cybersecurity Threats of 2023

March 28, 2023

Welcome



Hank Wolfson
Partner & Chief Operating Officer
Gray, Gray & Gray, LLP
hwolfson@gggllp.com

Today's Presenter



Nate Gravel, CISA, CISM, CRISC
Cybersecurity Consultant
Gray, Gray & Gray, LLP
ngravel@gggllp.com

Agenda

- Cybersecurity Threat Landscape
- Top Threats Facing Our Clients
 - Phishing
 - Malware/Ransomware
 - Business E-mail Compromise
- Mitigation Measures
- Q&A
- Closing Remarks



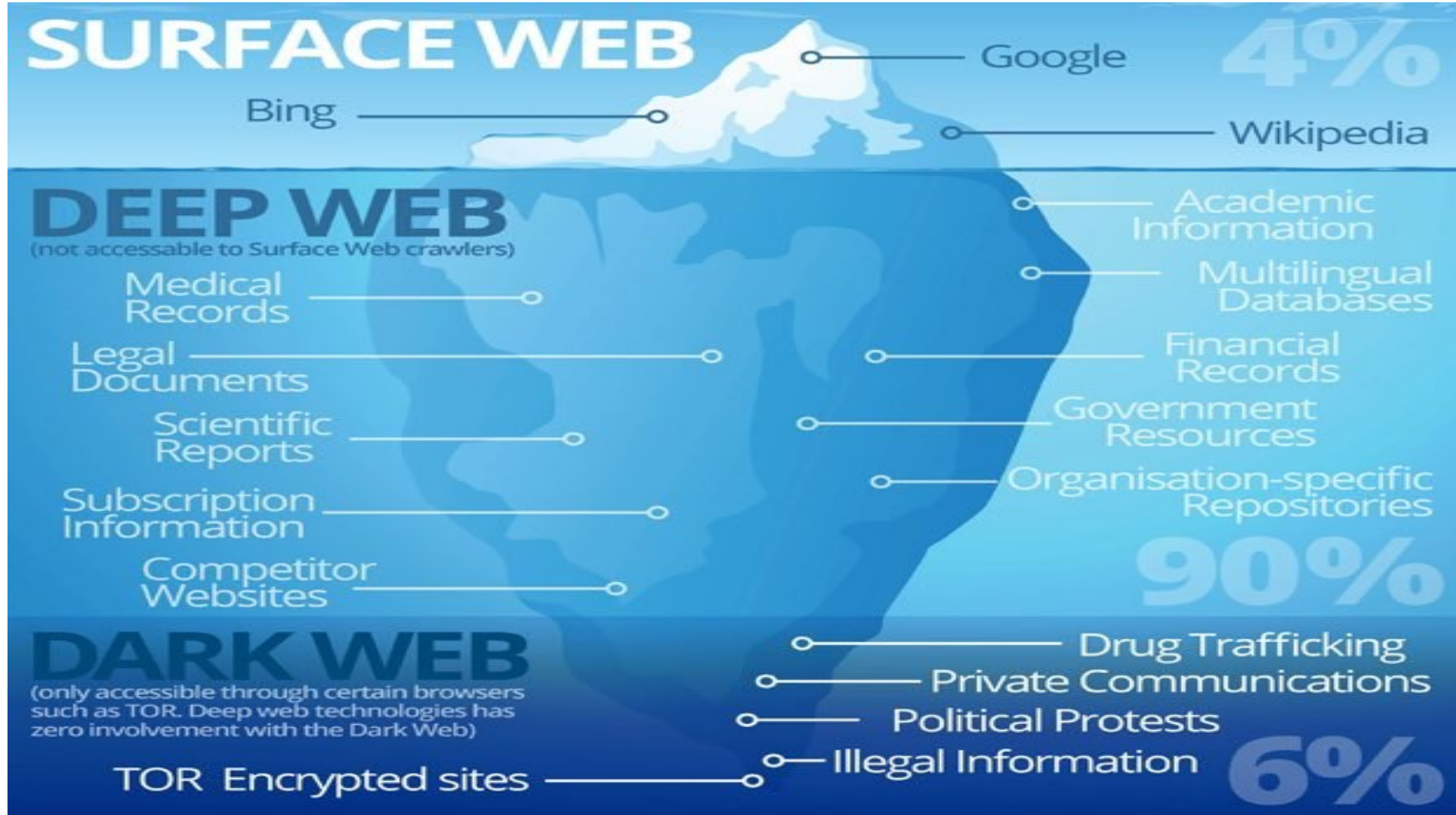
Poll Question #1

- **How confident are you in your organization's cybersecurity risk management and ability to recover quickly from a cyber attack?**
 - Highly Confident
 - Confident
 - Somewhat Confident
 - Not Confident
 - Unsure

The Cybercrime Landscape

According to some studies, the global cost of cybercrime is projected to reach over **\$10 trillion annually** by 2025.

The Cybercrime Landscape



The Cybercrime Landscape

Cybercrime is no longer a one man operation. Within the cybercrime underground an attacker can find a wealth of tools and services that can be bought or rented to facilitate different aspects of the attack lifecycle.*

Fraud as a service is constantly changing and adapting to new security solutions, offering end to end technologies, multiple SLA levels and low prices for everything a cybercriminal might need.

Malware

Cost: Free - \$20k (license based)

Trojan designed to steal data, manipulate online banking sessions, inject screens and more.



Exploit Kits

Cost: \$2K (monthly rental)

Toolkits designed to exploit system and software vulnerabilities resulting in a malicious download.



Droppers

Cost: Free - \$10K

Software designed to download malware to an infected device, evading antivirus and research tools.



Money Mules

Cost: Up to 60% of account balance

A person who receives the stolen money from a hacked account and transfers the funds via an anonymous payment service to the mule operator.



Infrastructure

Cost: \$50 - \$1,000 (Rental per month)

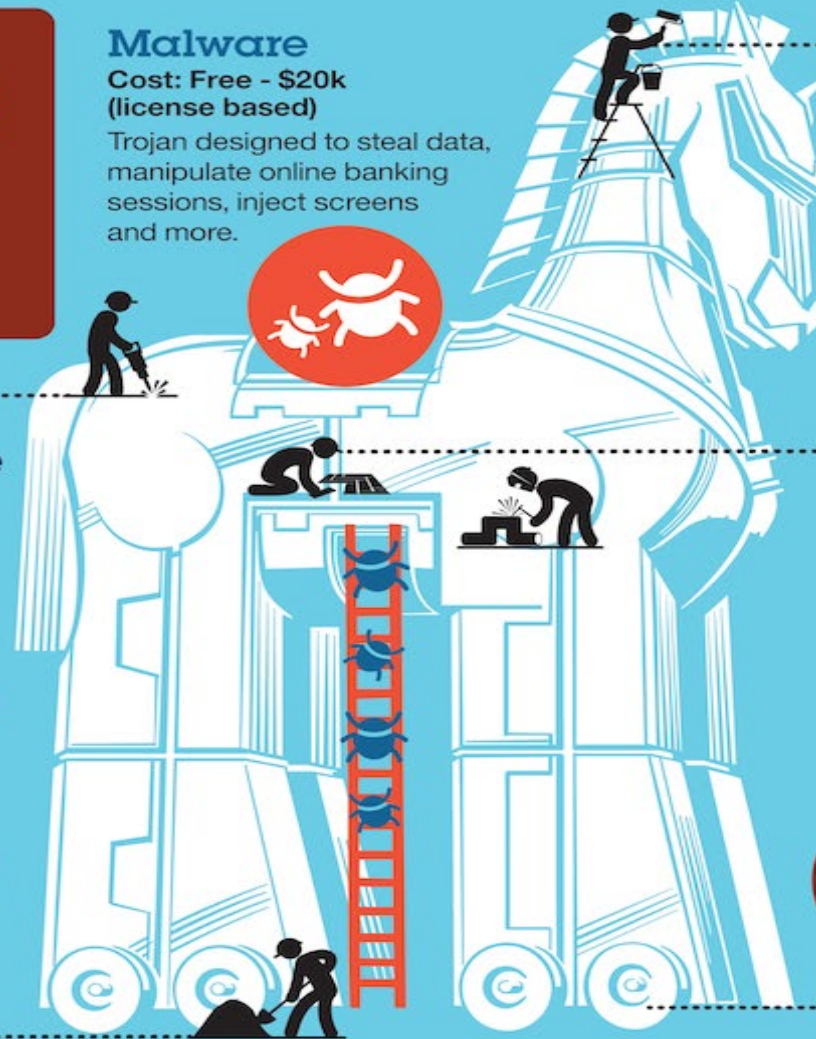
Hosting services for malware update, configuration and command and control servers. Some are fast flux or TOR based.



Spammers

Cost: \$1 - \$4 per 1000 emails

Spam botnet operators that spread emails with attachments or links leading to a Trojan infection.



* This infographic shows one possible scenario of a cybercriminal attack lifecycle. Prices for this scenario are estimates.

The Cybercrime Landscape

CVV FULLZ + ATM PIN (USA ONLY) 100% VALID

Vendor (4.60★) (a 951/20/47)

Price ₪0.01948 (\$75)

Ships to Worldwide, Worldwide

Ships from Worldwide

Escrow No

Image 1: A threat actor offers “cvv fullz + ATM PIN” on a Dark Web marketplace for \$75 USD.

ULTRA HQ USA FULLZ (DOB/MMN/BILL)

Vendor (4.68★) (a 0/0/0)

Price ₪0.002078 (\$8)

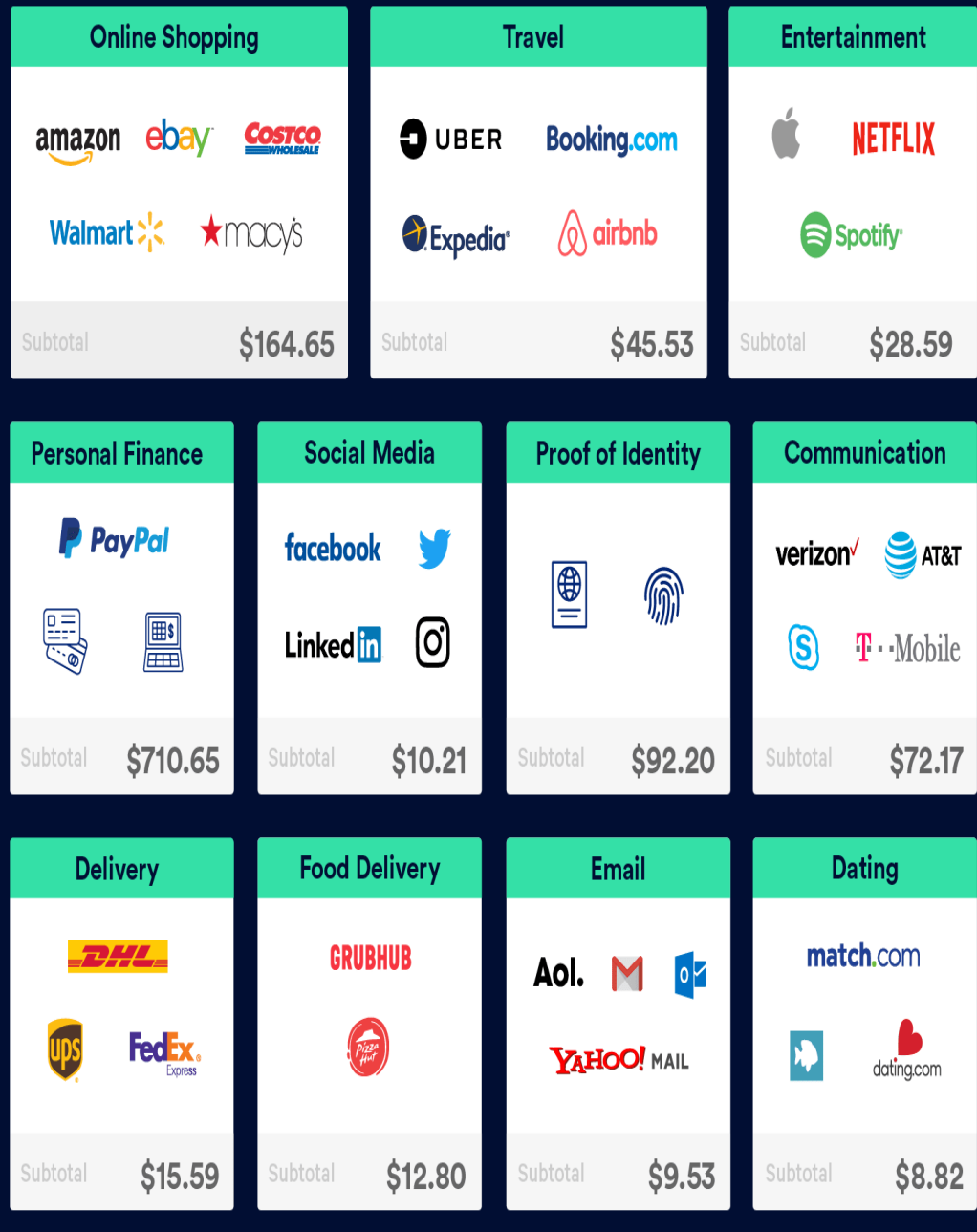
Ships to Worldwide, Worldwide

Ships from usa

Escrow Yes

Image 2: A threat actor offers fullz — including the victim’s date of birth, mother’s maiden name, and billing information — on a Dark Web marketplace for \$8 USD.

Brand	Level	Credit?	Tracks	SCode	Country	State	City	ZIP	Ref.?	Price
China Unionpay	Rewards	Credit	TR2	206	N/A	-	-	-[-]	Yes	\$5.00
Visa	Business	Credit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00
Visa	Classic	Debit	TR2	221	N/A	-	-	-[-]	Yes	\$5.00
Amex	Green	Credit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00
Mastercard	Standard	Debit	TR2	221	N/A	-	-	-[-]	Yes	\$5.00
China Unionpay	Rewards	Credit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00
Visa	Classic	Credit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00
Visa	Classic	Debit	TR2	226	N/A	-	-	-[-]	Yes	\$5.00
Mastercard	Standard	Debit	TR2	221	N/A	-	-	-[-]	Yes	\$5.00
Visa	Gold	Credit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00
Mastercard	Standard	Debit	TR2	221	N/A	-	-	-[-]	Yes	\$5.00
Mastercard	Standard	Debit	TR2	221	N/A	-	-	-[-]	Yes	\$5.00
Discover	Standard	Debit	TR2	221	N/A	-	-	-[-]	Yes	\$5.00
Visa	Signature	Credit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00
China Unionpay	Standard	Debit	TR2	220	N/A	-	-	-[-]	Yes	\$5.00
Mastercard	Standard	Debit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00
Mastercard	Standard	Debit	TR2	221	N/A	-	-	-[-]	Yes	\$5.00
Amex	Gold	Credit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00
China Unionpay	Rewards	Credit	TR2	206	N/A	-	-	-[-]	Yes	\$5.00
China Unionpay	Electron	Debit	TR2	221	N/A	-	-	-[-]	Yes	\$5.00
Visa	Classic	Credit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00
Visa	Platinum	Credit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00
China Unionpay	Standard	Debit	TR2	221	N/A	-	-	-[-]	Yes	\$5.00
Visa	Classic	Credit	TR2	201	N/A	-	-	-[-]	Yes	\$5.00



The Cybercrime Landscape

The average consumer is worth about **\$1,200** on the Dark Web.

Top Threats Facing Our Clients



Phishing



Business E-mail Compromise



Malware
(Ransomware)

Poll Question #2

- Does your organization leverage a cybersecurity awareness employee training program such as KnowBe4?
 - Yes
 - No
 - Unsure


Phishing



Debbie [redacted] <debbiea@[redacted].com>

FW: Transfer

To Nathaniel C. Gravel

Message  CSKX Wire Instructions.pdf (122 KB)

From: Lee [redacted] [[mailto:lee@\[redacted\].com](mailto:lee@[redacted].com)]

Sent: Wednesday, August 26, 2015 1:01 PM

To: Debbie [redacted]

Subject: RE: Transfer

Please go to the bank and make a transfer for \$104,549.36 and the purpose for the wire is Admin services. Send me the confirmation once done.

Lee

Lee [redacted]

On 2015-08-26 16:42, Debbie [redacted] wrote:

I can go to the bank and see.

[mailto:lee@\[redacted\].com](mailto:lee@[redacted].com)

Debbie

Phishing

Top spoofed brands year over year

	2022	2021
1	Microsoft	Microsoft
2	Google	Apple
3	Yahoo	Google
4	Facebook	BMO Harris Bank
5	Outlook	Chase
6	Apple	Amazon
7	Adobe	Dropbox
8	AOL	DHL
9	PayPal	CNN
10	Office365	Hotmail

41%

Percentage of incidents involving phishing for initial access

Phishing operations continued to be the top pathway to compromise in 2022, with 41% of incidents remediated by X-Force using this technique to gain initial access.

62%

Percentage of phishing attacks using spear phishing attachments

Attackers preferred weaponized attachments, deployed by themselves or in combination with links or spear phishing via service.

Phishing (Smishing)

(ALERT!) Your Bmo Bank account has been suspended. To unlock your account, click here: <https://bit.ly/1EeZ6m2>

John, transfer €300k to the following a/c. No time to explain just do it and I'll explain after the board meet.

Is this really a pic of you?
<http://tinyurl.com/ntn9ohk>

Dear Customer,

Your AppleID is due to expire Today, Please tap <http://bit.do/cRqb6> to update and prevent loss of services and data.

Apple smsSTOPto43420

Dear Walmart shopper, your purchase last month won a \$1000 Walmart Gift Card. Click here to claim:
www.WmartProgram.com
(Quit2end)

Dear NAB Bank User, We have detected some unusual activity. We urgently ask you to follow the account review link:
<http://bit.do/nab-bank>

Poll Question #3

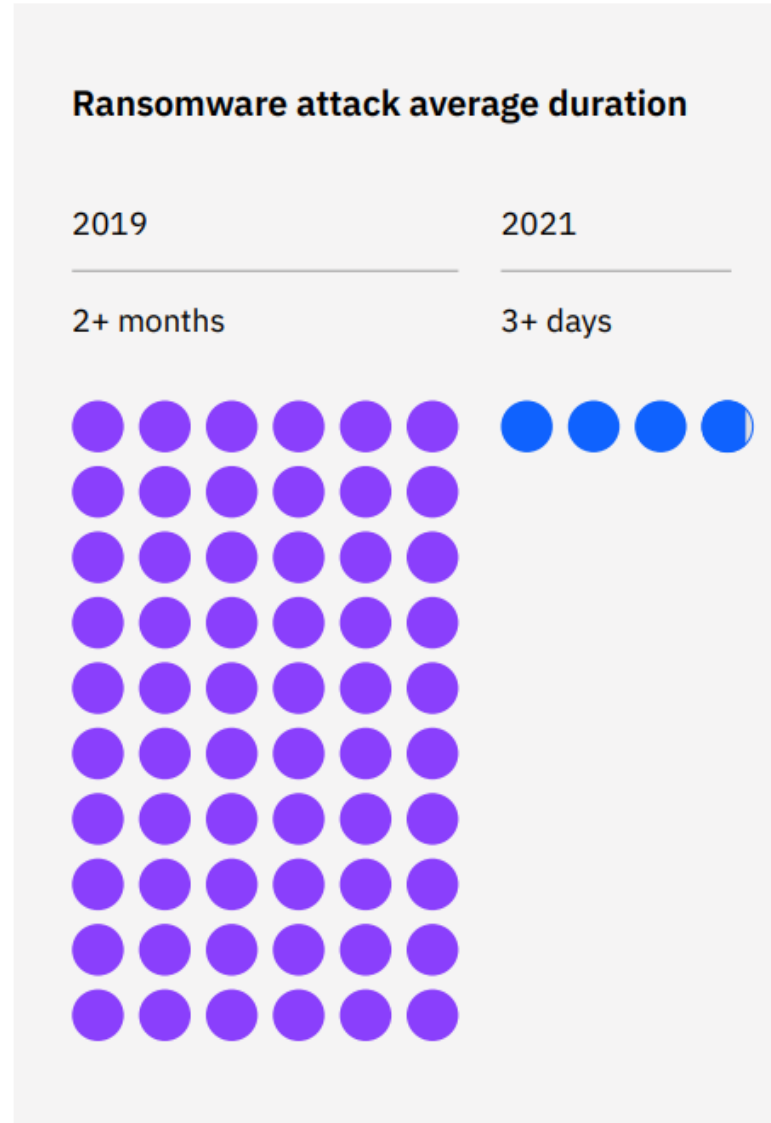
- Has your organization ever hired a third party to conduct a vulnerability assessment and/or penetration test?
 - Yes
 - No
 - Unsure

Malware/Ransomware

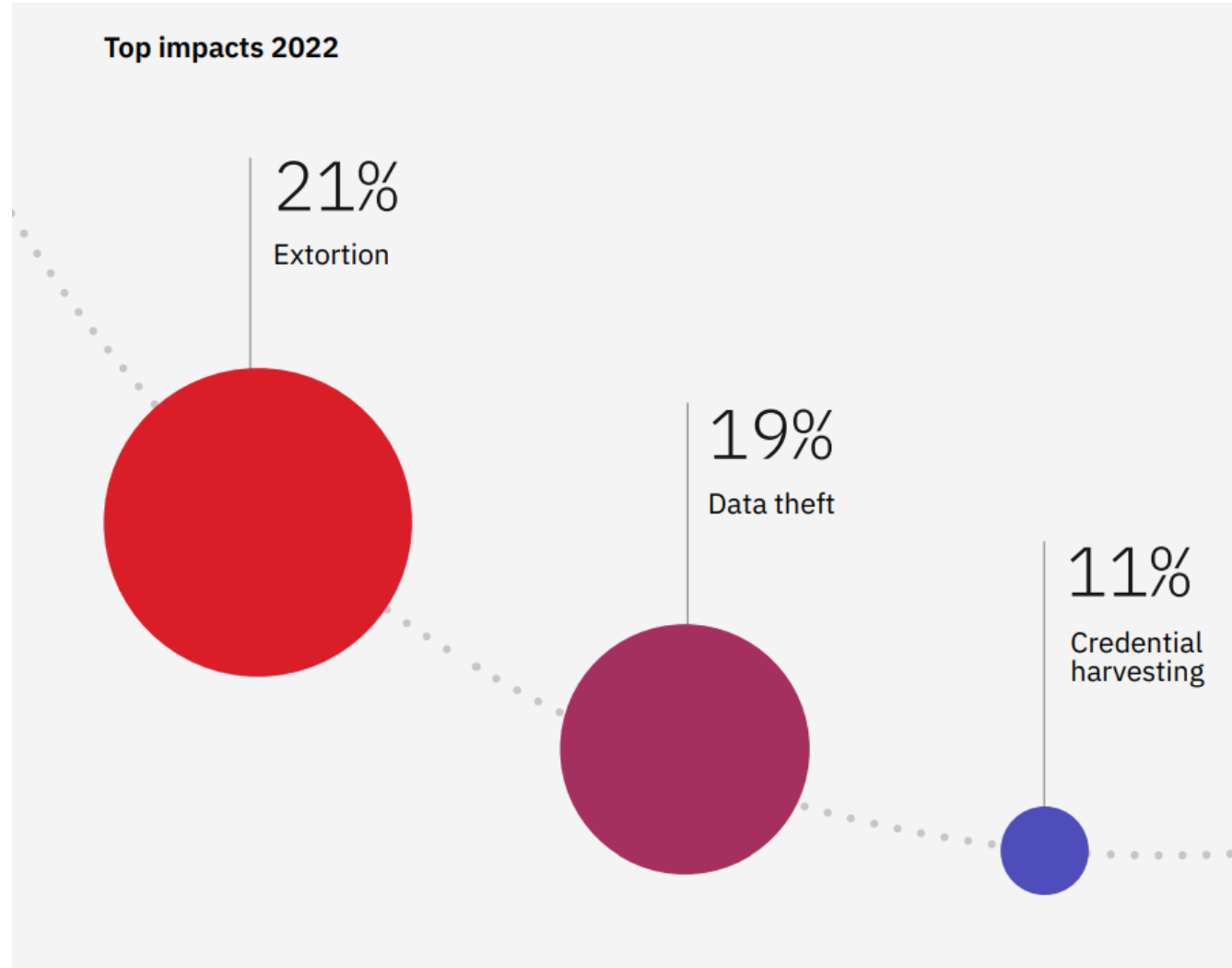
55% OF SMALL BUSINESSES pay hackers the ransom

- RANSOMWARE 2.0**
- Destroys backups
 - Steals credentials
 - Publicly exposes victims
 - Leaks stolen data
 - Threatens victim's customers

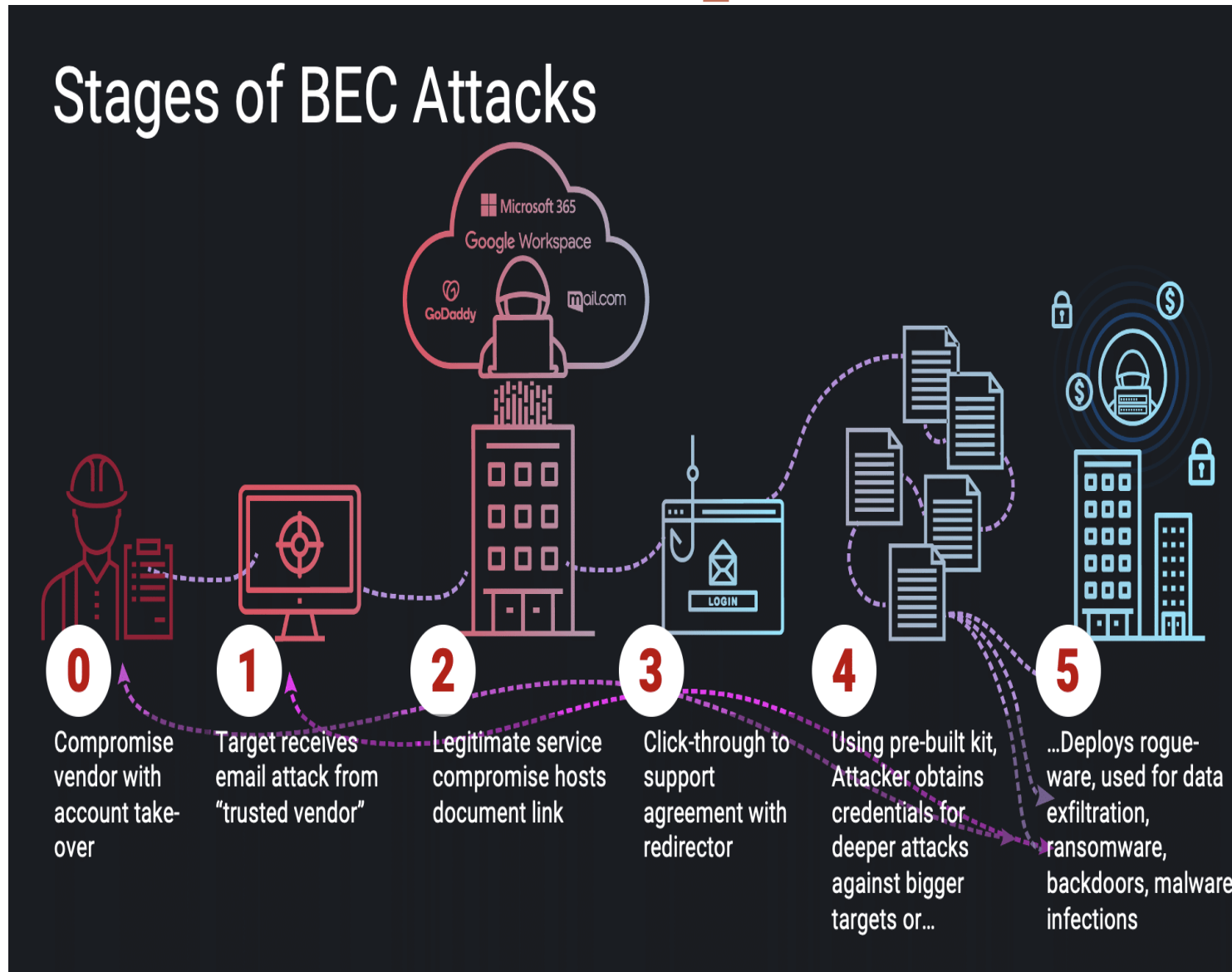
RANSOMWARE ATTACKS A COMPANY EVERY **14 SECONDS**



Malware/Ransomware



Business E-mail Compromise



Credential Theft/Account Takeover

';--have i been pwned?

Check if your email or phone is in a data breach

ngravel@gravoc.com

pwned?

Oh no — pwned!

Pwned in 10 [data breaches](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)



ParkMobile: In March 2021, the mobile parking app service ParkMobile suffered a data breach which exposed 21 million customers' personal data. The impacted data included email addresses, names, phone numbers, vehicle licence plates and passwords stored as bcrypt hashes. The following month, the data appeared on a public hacking forum where it was extensively redistributed.

Compromised data: Email addresses, Licence plates, Names, Passwords, Phone numbers

Poll Question #4

- How often does your organization conduct an assessment of its cybersecurity risk controls
 - Annually
 - Semi-annually
 - Quarterly
 - Monthly
 - Never
 - Unsure

Mitigation Measures: Our Advice to All Clients



- Perform Risk Assessment/Gap Analysis
 - Assess Security Operations (People, Process, Technology)
 - Assess Administrative, Physical, & Technical Controls
- Perform Vulnerability Assessment/Penetration Testing
 - Internal/External Network
 - Cloud Services (Office 365, etc.)
- Perform Social Engineering Exercise
 - Simulated Phishing
 - Simulated Spear Phishing

Mitigation Measures: Our Advice to All Clients



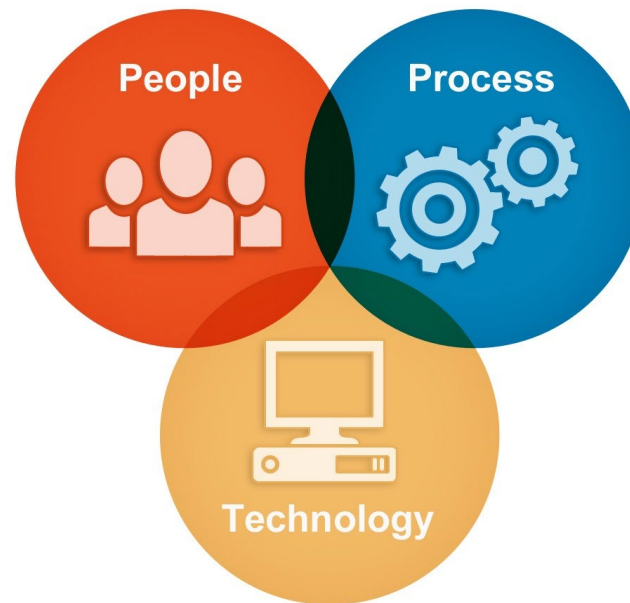
1. Train/educate
2. Invest in all 3 core components of security posture: protection, detection, response
3. Test (retest) and don't be afraid to fail

Question & Answer



Closing Remarks

Information security is **people**, **process**, and **technology**, not firewalls, encryption, and antivirus.



Thank you



Hank Wolfson
Partner & Chief Operating Officer
Gray, Gray & Gray, LLP
hwolfson@gggllp.com
781.407.0300



Nate Gravel, CISA, CISM, CRISC
Cybersecurity Consultant
Gray, Gray & Gray, LLP
ngravel@gggllp.com
781.407.0300