

Cybersecurity Hot Topics

The Latest Trends

April 20, 2022

wipfli.com

WIPFLI



Contact Information



Mark Scholl

Principal

Wipfli LLP

815.626.1277

mscholl@wipfli.com

Certified Ethical Hacker (CEH)

Certified Information Systems Auditor (CISA)

Certified Information Systems Security
Professional (CISSP)

Microsoft Certified Systems Engineer (MCSE)

Agenda:

Cybersecurity Trends

Risk Management

Resources



WIPFLI

Cybersecurity Trends

A blue-tinted photograph of a modern office interior. In the foreground, a man in a dark sweater and a woman in a white shirt are standing and talking; the man is holding a tablet. In the background, other people are seated at desks, some working on laptops. The office has large windows and a clean, professional look.

Cybersecurity threats and trends – Overview

- Threat actors are interested in you – everyone is a target
 - ▶ Small business, large business, individuals...
- Phishing and spam continue to be the most opportunistic attacks
- Digital extortion continues to be a significant threat
 - ▶ Primarily ransomware



Cybersecurity threats and trends – Threat actors

2021 Verizon Cyber Espionage Report

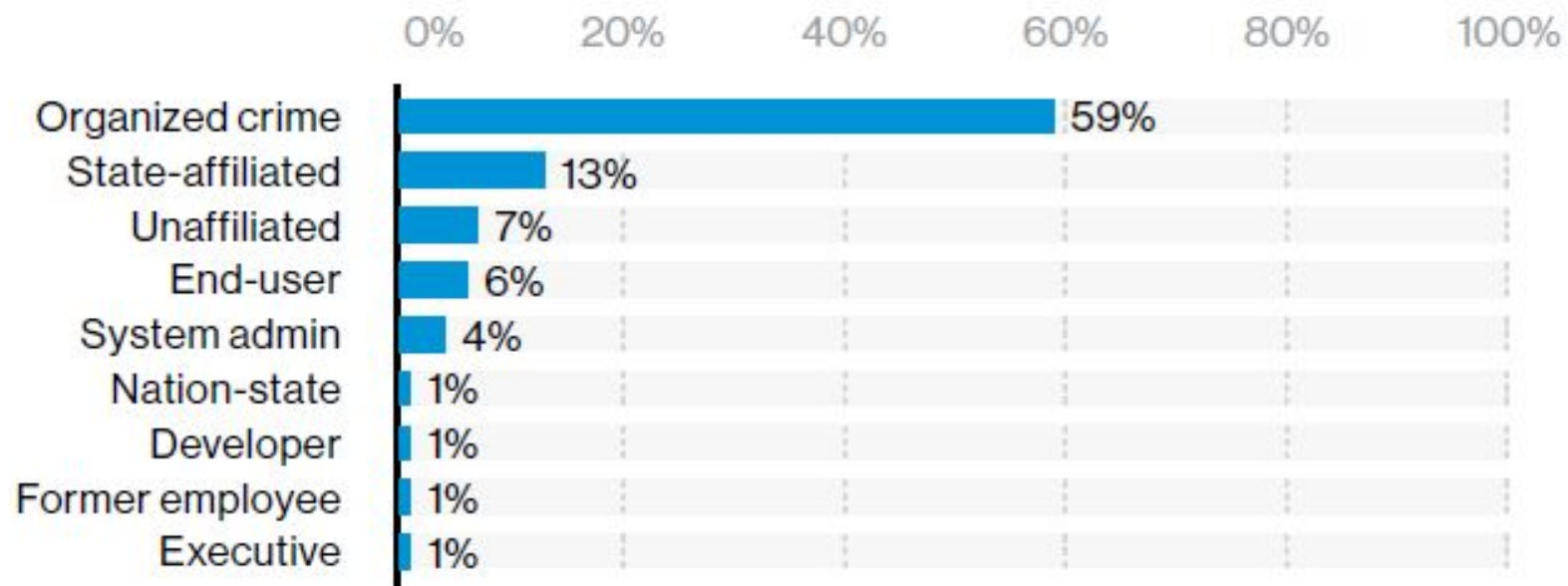


Figure #35: Actor varieties within all breaches (2014-2020 DBIR; n=9,077)

Cybersecurity threats and trends – State sponsored



WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

 Yuri Sergeevich Andrienko	 Sergey Vladimirovich Detistov	 Pavel Valeryevich Frolov
 Anatoliy Sergeevich Kovalev	 Artem Valeryevich Ochichenko	 Petr Nikolayevich Pliskin

Challenges for law enforcement

- Anonymity
 - ▶ Originating IP address is difficult to track
 - ▶ Dark web users do not use nicknames, usernames, or email addresses from surface web
- Jurisdictional
 - ▶ Extradition rights
 - ▶ Digital crime continues to evolve
- Money trail
 - ▶ Cryptocurrencies

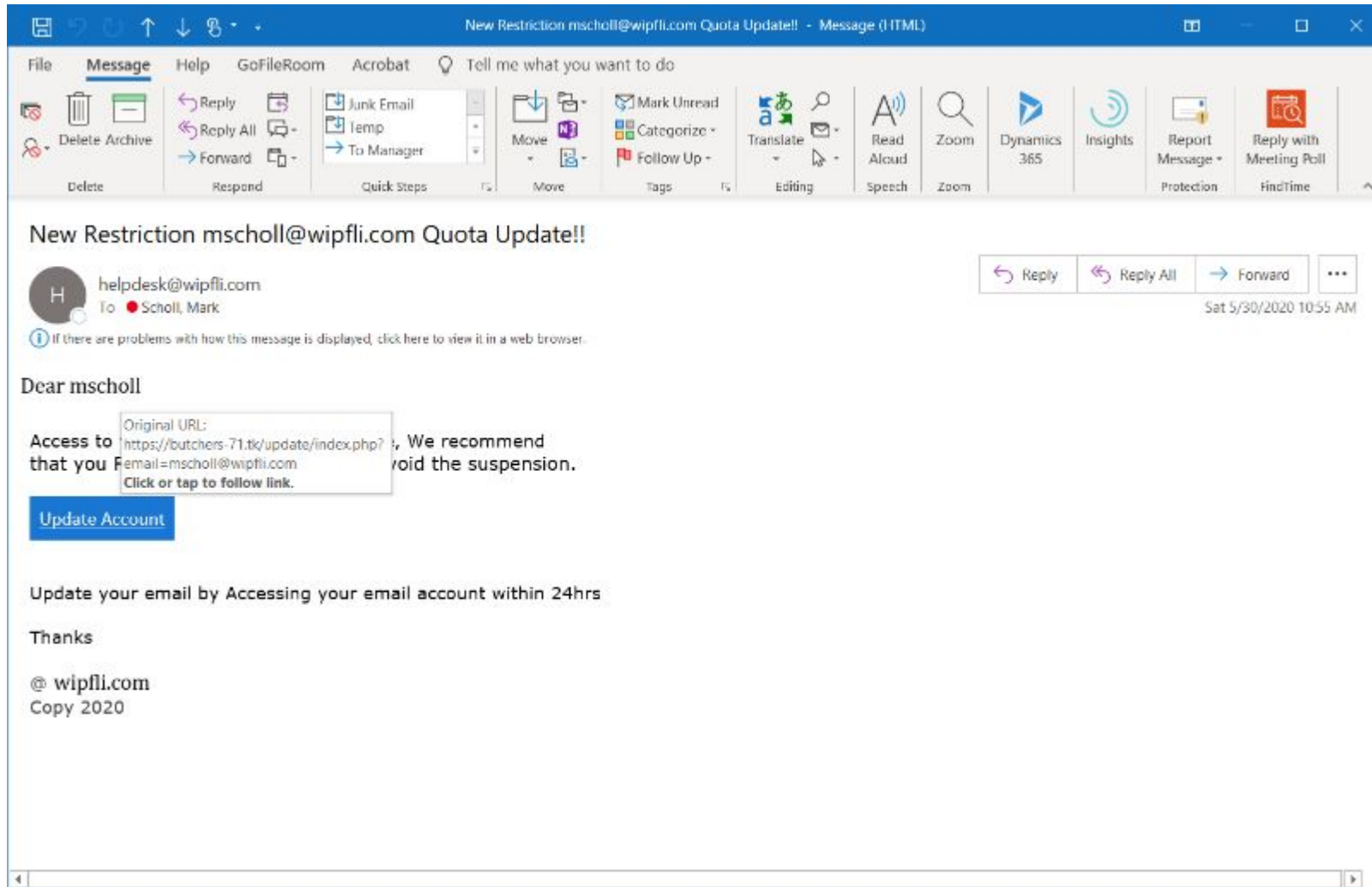


Cybersecurity threats and trends – Email scam types



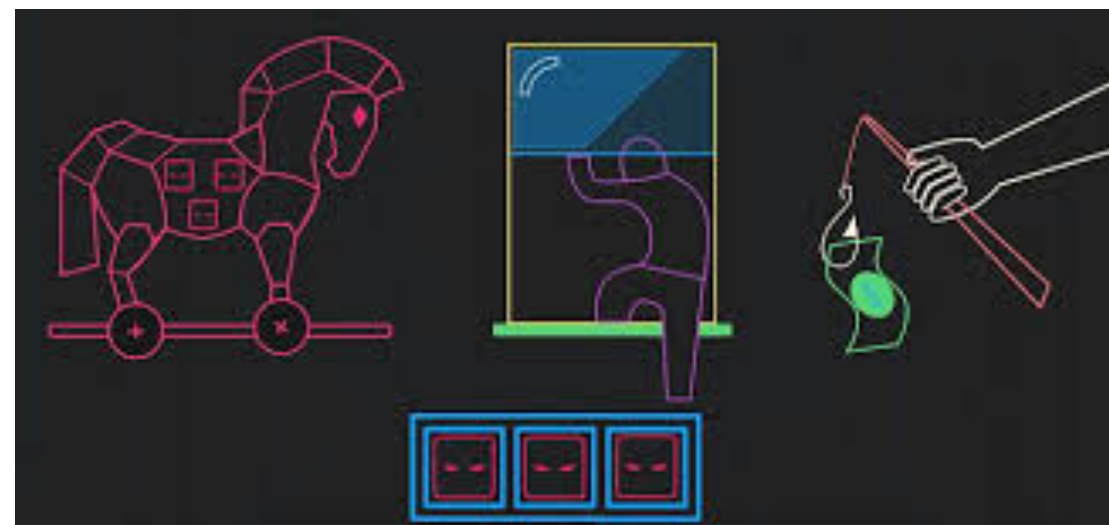
- Email scams are the attack vector!!!
 - ▶ Deliver malicious software
 - Ransomware
 - Backdoors
 - Keyloggers
 - ▶ Account takeover
 - ▶ Business email compromise (BEC)
 - ▶ Extortion

Email phishing example – Password stealing



Supply chain attacks

- Emerging threat that targets software developers and suppliers
- Outside partner or provider with access to your system is infiltrated
 - ▶ **Process of infecting legitimate applications**
 - Accessing and modifying source code
 - Typically installed through application updates
 - ▶ **Examples**
 - SolarWinds attack
 - Kaseya
 - Log4j
 - **Open-source software libraries**



Cybersecurity trends – Business email compromise (BEC)

- Attacker targets CxO or business owner; attacker gains access to victim's email account or uses a “look-alike” domain to send a message tricking an employee into performing a wire transfer or other identity scam
 - ▶ Fraudulent wire transfer
 - ▶ Payroll diversion
 - ▶ Gift card scam
 - ▶ Tech support scam
 - ▶ W-2 scams



Business email compromise

From: [REDACTED]
Date: March 23, 2016 at 10:25:39 AM CDT
To: [REDACTED]
Subject: Wire Payment



Mark,

Are you in the office? I'm in a contract meeting til 5pm and i need you to take care of an invoice payment before the cutoff time today.

I'm very busy, Email me.

[REDACTED]

Chairman Emeritus

[REDACTED]

Phone [REDACTED]

Fax [REDACTED]

[REDACTED]

Evolution of ransomware – Dual threat

- Encrypt organization's data and require ransom to be paid for encryption key
 - ▶ Backup for recovery as a reactive control
- Name and shame
 - ▶ Threat of leaking the organization's data on the internet
- Average downtime of a ransomware attack is 19 days
- Extortion demands have drastically increased – many are demanding six-figure sums to release the data

Evolution of ransomware – Dual threat

The image shows a ransomware payment screen with a blue background. At the top, there is a barcode with the word "T E S L A C R Y P T" underneath it. Below the barcode, the text reads "All your important files are encrypted." followed by "At the moment, the cost of private key for decrypting your files is 1.5 BTC ≈ 415 USD." and "Your Bitcoin address for payment: 1LvjW9wyajpsC3j9RitZDip6cDcZ7jjMG5". There are two buttons: "PURCHASE PRIVATE KEY WITH BITCOIN" and "PURCHASE PRIVATE KEY WITH PAYSAFECARD OR UKASH". Below the second button, it says "You can also make a payment with PaySafeCard or Ukash" and "In case of payment with PaySafeCard or Ukash your total payment is £ 400". A note at the bottom of the blue section says "Payment verification may take up to 12 hours." The bottom section is white and contains a red-bordered box around the text "Support Message Center". Below this, it says "Try to decrypt your file here" and "You can test the decryption service once for FREE." There is an input field and a "Browse..." button at the bottom.



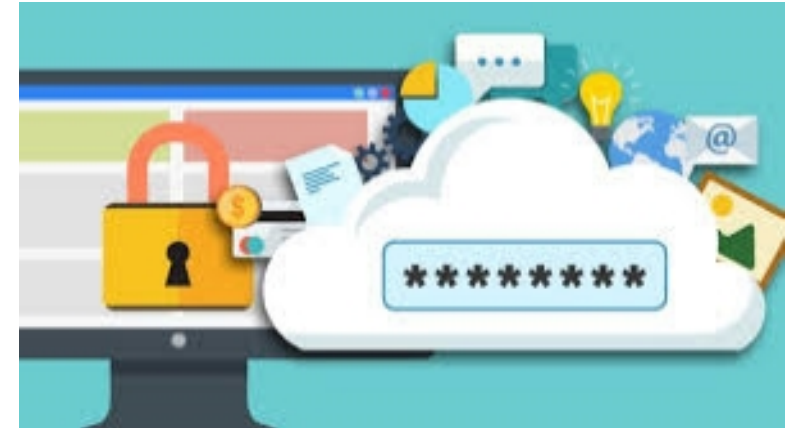
Risk Management

Cybersecurity key controls

- Focus on the basics
 - ▶ Patch management, perimeter defense, encryption, backups
 - ▶ Access control management, inventory of hardware/software
 - ▶ Network monitoring, malware protection, network segmentation
- Talk with your internet service provider and vendors about DDoS attacks
- Ongoing employee training and testing

Strong Authentication

- Passwords should be minimum length of 14 characters
- Multi-factor authentication
 - ▶ Remote access
 - ▶ Administrative accounts
- Password managers
 - ▶ Generates strong and unique passwords
 - ▶ Auto-fill logins
 - ▶ Provides security score for “at-risk” passwords
 - ▶ Notifies you of any login credentials involved in a data breach



Cyber incident management and resilience

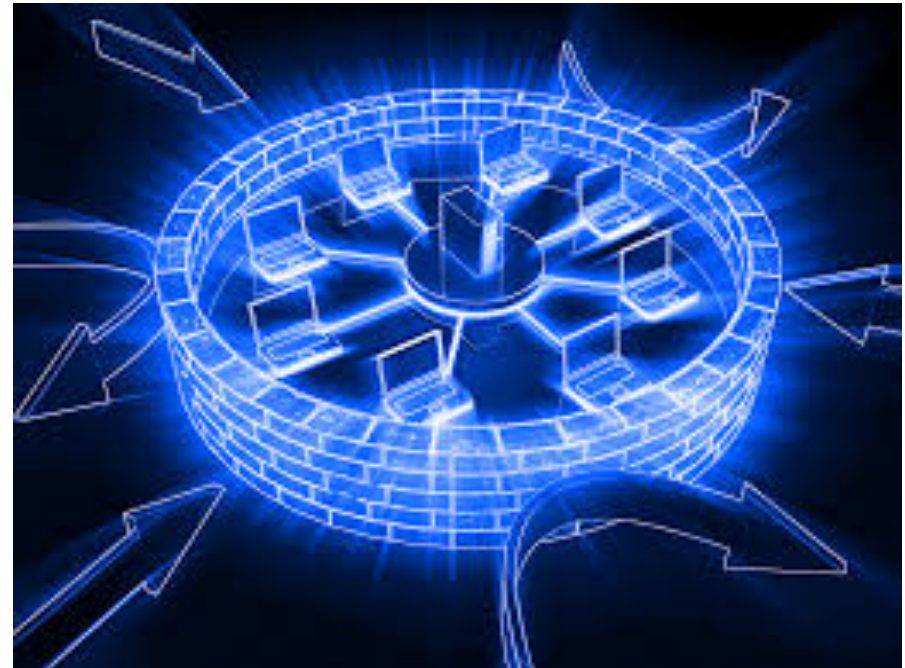
- Create a positive cybersecurity culture
- Have enhanced incident response plans – tabletop testing
 - ▶ Have arrangements with vendors who can work with your institution to implement incident response—a proactive approach, not when an incident has occurred
 - ▶ Work with regional crime taskforces
 - ▶ Ensure plan includes how you will notify customers
- Ensure there is periodic tabletop testing of your incident response program

Cybersecurity insurance

- Fee is increasing mostly due to ransomware attacks (15% is the beginning range in many instances)
 - ▶ Drastic increase in extortion demands
 - ▶ Mandated notifications
- Understand your data collection and protection requirements
 - ▶ Multi-factor authentication
 - ▶ Security monitoring
- Pay attention to exclusionary language

Validating your controls

- IT controls review
- Penetration testing
- Vulnerability assessments
- Cloud security assessments
 - ▶ M365, AWA, Azure
- Social engineering
 - ▶ Email spoofing
 - ▶ Pretext calling
 - ▶ Onsite physical pen testing





Resources

Cybersecurity resources

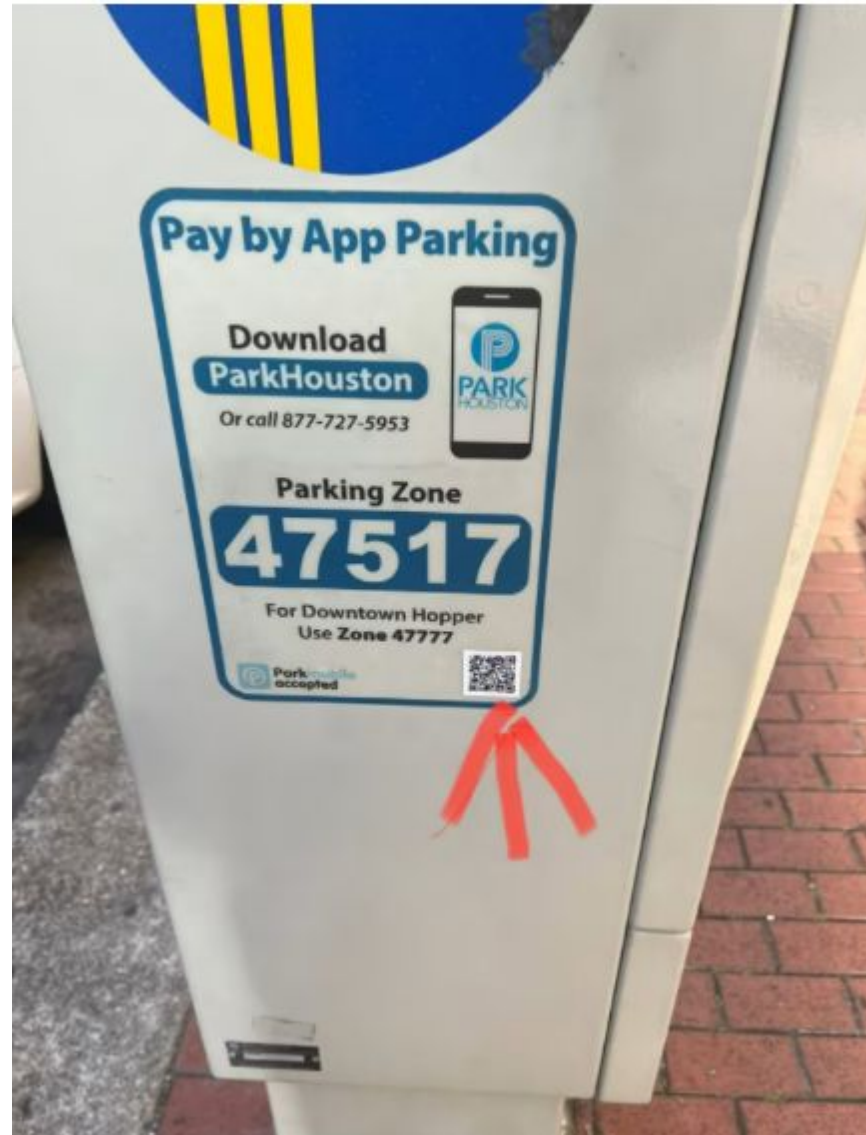
- 18 CIS Critical Security Controls
 - ▶ <https://www.cisecurity.org/controls/cis-controls-list>
- Ransomware Self-Assessment Tool
 - ▶ <https://www.csbs.org/ransomware-self-assessment-tool>
- Regulatory bulletins and alerts
 - ▶ US-CERT
 - <https://www.cisa.gov/uscert/mailing-lists-and-feeds>
- Shields Up
 - ▶ <https://www.cisa.gov/shields-up>

InfraGard

- www.infragard.org
- Partnership between the FBI and members of the private sector
- Provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure



QR code phishing



QR code phishing

- One is good and one is bad... Do you know the difference?



QR code phishing

Good

www.chicagocubs.com



Bad!!!

www.stlouiscardinals.com



QR code phishing

- Treat them the same way as links in emails.
 - ▶ Is it taking you to a website you were expecting? Does it look as it should?
 - ▶ Use a clean browser and type in the web address manually before logging in or making a payment
- Think before you scan. Is it a sticker? Is it in an email?
- A password manager can be helpful to spot websites that do not represent the legitimate site.
- Use QR code scanning apps that filter phishing sites.

Questions?