PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

2023 Nonprofit Symposium:
Managing Cybersecurity and Privacy Risks of a Nonprofit

Thomas J. DeMayo, CISSP, CIPP, CEH, CPT, CISA, CRISC
Partner, Cybersecurity and Privacy Advisory

Alexander K. Buchholz, CPA, MBA, CGMA
Partner, Nonprofit Services

KNOW
GREATER
VALUE®

December 12, 2023

Biography

Thomas DeMayo CISSP, CISA, CIPP/US, CPT, CEH, CCFE, CHFI, CRISC, CMMC-CCP, CDPSE is the Partner-in-Charge of the PKF O'Connor Davies Cyber Risk and Privacy Group. In this role he is responsible for the implementation and design of the Firm's cybersecurity service offerings, and internal/external audit programs and testing procedures. He is the Firm's leader relating to cybersecurity, information security, governance, privacy, incident response, business continuity and disaster recovery and computer forensics

Biography

Alexander K. Buchholz is a Partner at PKF O'Connor Davies LLP with more than 20 years of experience in public accounting, including with a "Big Four" accounting firm. Alex's expertise is in Single Audits and internal control/compliance audits. His industry experience is in Not-for-Profit entities and healthcare and, including skilled nursing facilities, social service agencies, charter schools, diagnostic and treatment centers, home care service entities, adult homes and other long-term care facilities as well as special needs entities and cemeteries.

Alex is also an adjunct professor at Brooklyn College and Lehman College of the City University of New York in the Department of Accounting where he teaches undergraduate and graduate courses in accounting and auditing.

He conducts internal training seminars for the Firm and frequently speaks to outside organizations and associations. He is also a former member of the Firm's continuing professional education (CPE) committee, with special emphasis on Single Audit training. Alex also writes various articles on accounting and auditing topics for a variety of professional publications.

Biography *(continued)*

Professional Affiliations & Civic Involvement

American Institute of Certified Public Accountants (AICPA)

New York State Society of Certified Public Accountants (NYSSCPA)

- Former Chair, Academic Advancement of Higher Education
- Former Member and Chair, Health Care Committee
- Former Member, Not-for-Profit Committee
- Former Member, Foundation for Accounting Education

New Jersey Society of Certified Public Accountants

- Nonprofit Interest Group

George Washington Society of Certified Public Accountants

- Nonprofit Interest Group

National Conference of CPA Practitioners

New York State Association of Cemeteries

Metropolitan Cemetery Association

Board Member, St. Mary's Healthcare System for Children

Board Member, New York State Board of Public Accountancy

Board Member and Audit Committee Chair, American Academy McAllister Institute of Funeral Services, Inc.

Presentation Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the participant individually and, unless expressly stated to the contrary, are not the opinion or position of the New York State Board of Public Accountancy and / or PKF O'Connor Davies, LLP.

Overview of PKF O’Connor Davies, LLP

- Founded in 1891
- Eighteen office locations in the following states: New York, New Jersey, Connecticut, Rhode Island, Maryland, Florida and Massachusetts, and internationally in India, with more than 1,400 professionals led by 150 partners
- Partners – 220
- Employees - 1200
- 12th Largest Accounting Firm in the NY Metropolitan area
- 25th Largest Accounting firm Nationwide
- Lead North American firm of PKF International, a global network of independent accounting and advisory firms

Cybersecurity is Business Risk

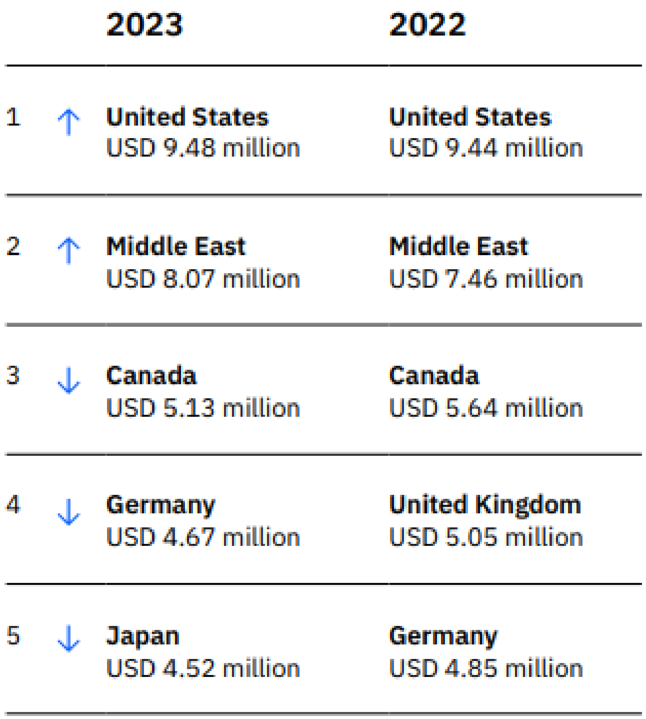
- Implications for not managing the risk
  - Financial
  - Operational – Loss of data
  - Productivity loss
  - Regulatory
  - Reputational – Loss of trust by employees, donors, customers, regulators
- The responsibility of managing the risk is owned by the Business, not IT.
  - Cybersecurity is a business issue that requires the assistance of a technical solution.

Cyber Statistics

- Global cybercrime costs are projected to rise to $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. (Cybersecurity Ventures)
- Eighty-three percent of breaches are initiated by external attackers. (Verizon)
- Eighty-four percent of breaches target humans as the attack vector, using social engineering and BEC strategies. (Verizon)
- As of 2023, the global average cost per data breach amounted to 4.45 million. (IBM)
- Globally, companies take 204 days to identify and 73 days to contain a breach. (IBM)

Cyber Statistics

- Cost of a data breach by country

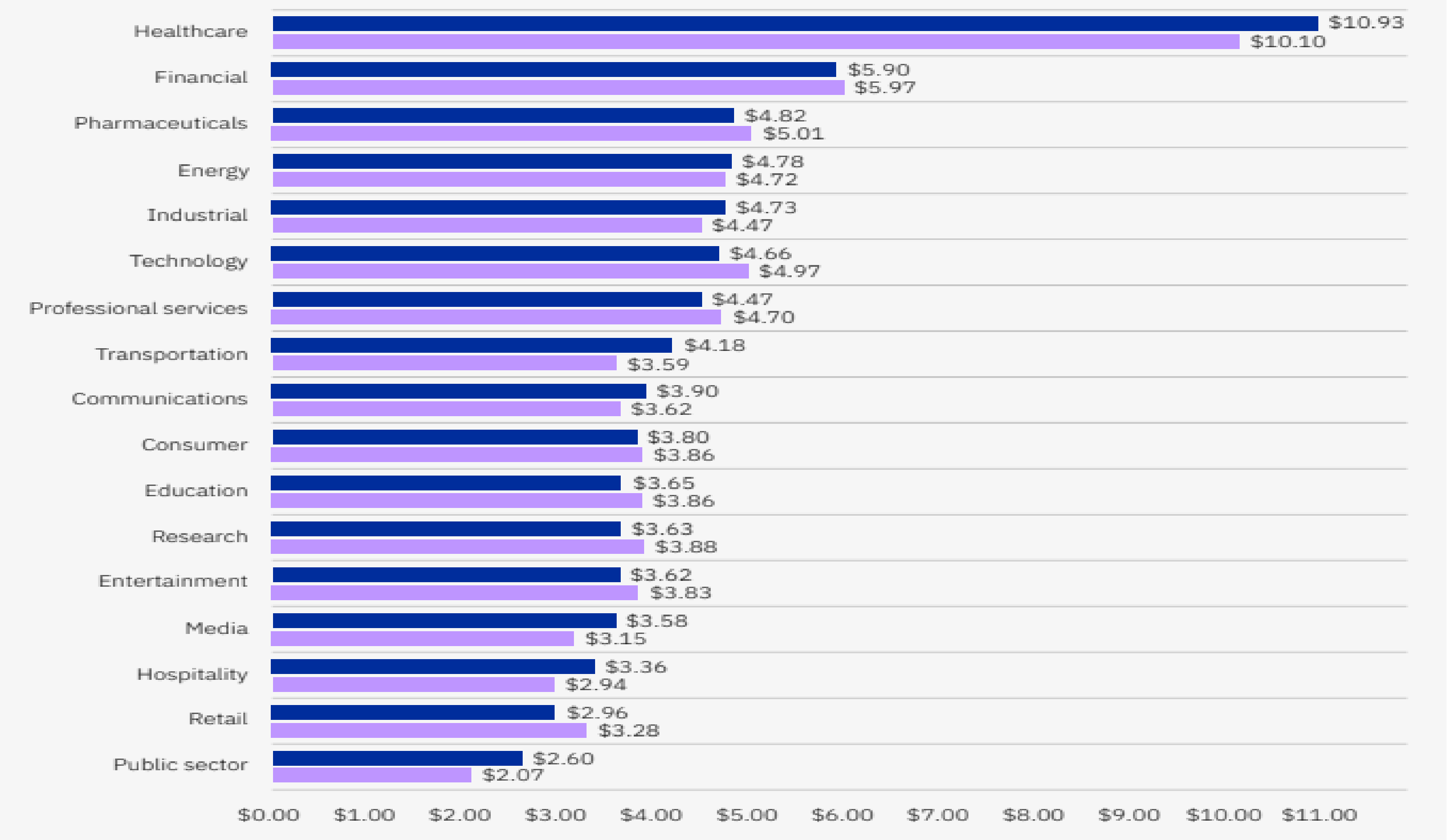


		2023	2022
1	↑	**United States** USD 9.48 million	**United States** USD 9.44 million
2	↑	**Middle East** USD 8.07 million	**Middle East** USD 7.46 million
3	↓	**Canada** USD 5.13 million	**Canada** USD 5.64 million
4	↓	**Germany** USD 4.67 million	**United Kingdom** USD 5.05 million
5	↓	**Japan** USD 4.52 million	**Germany** USD 4.85 million

Source: IBM

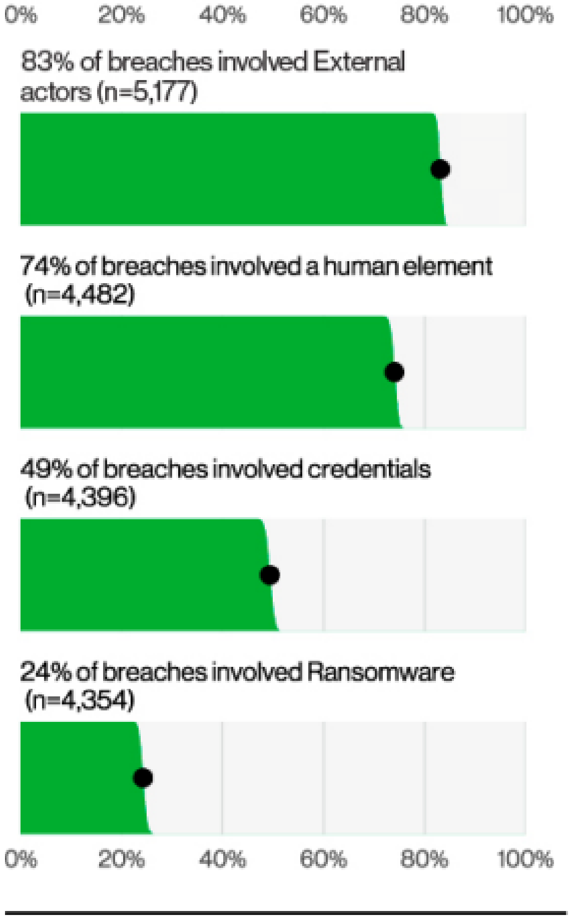
Cyber Statistics

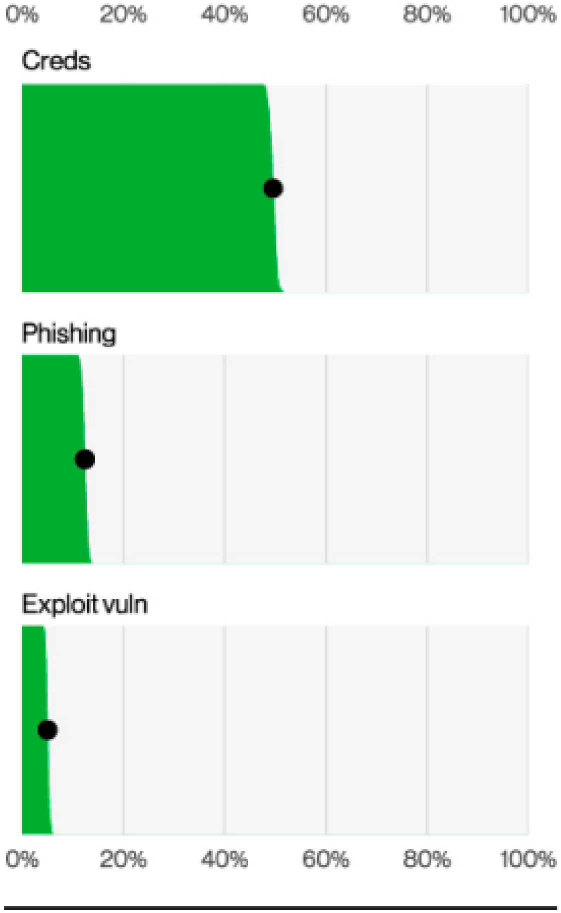
- Cost by Industry



Source: IBM

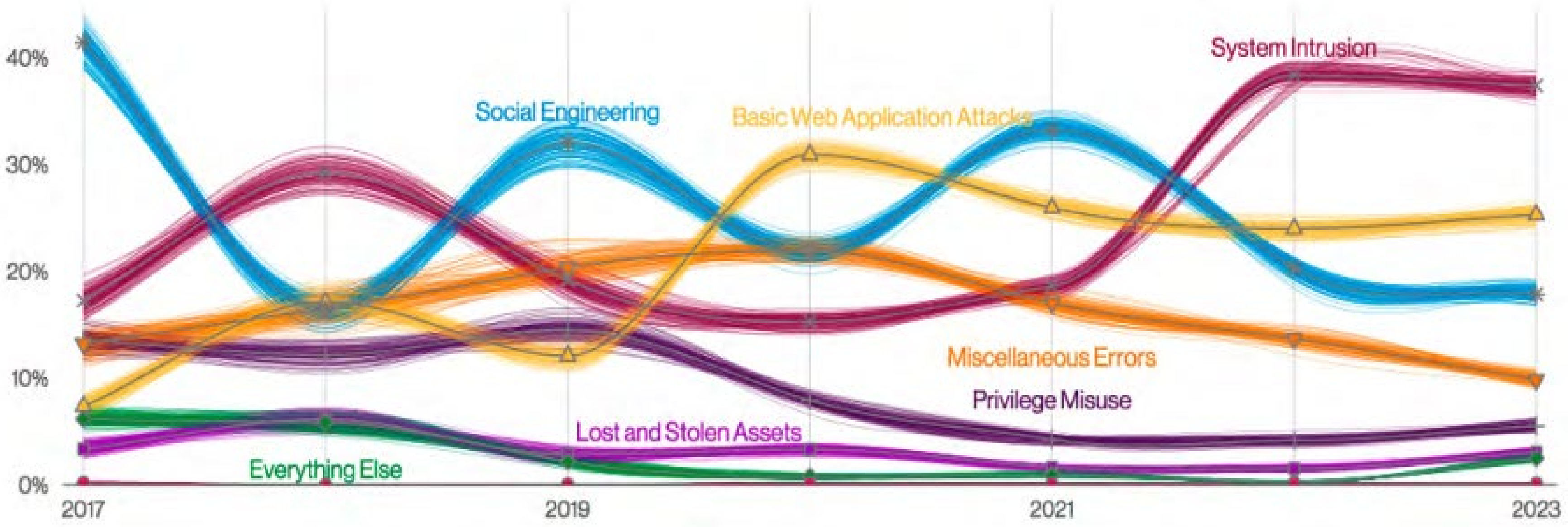
Attack Sources





Source: Verizon

Attack Sources



Source: Verizon

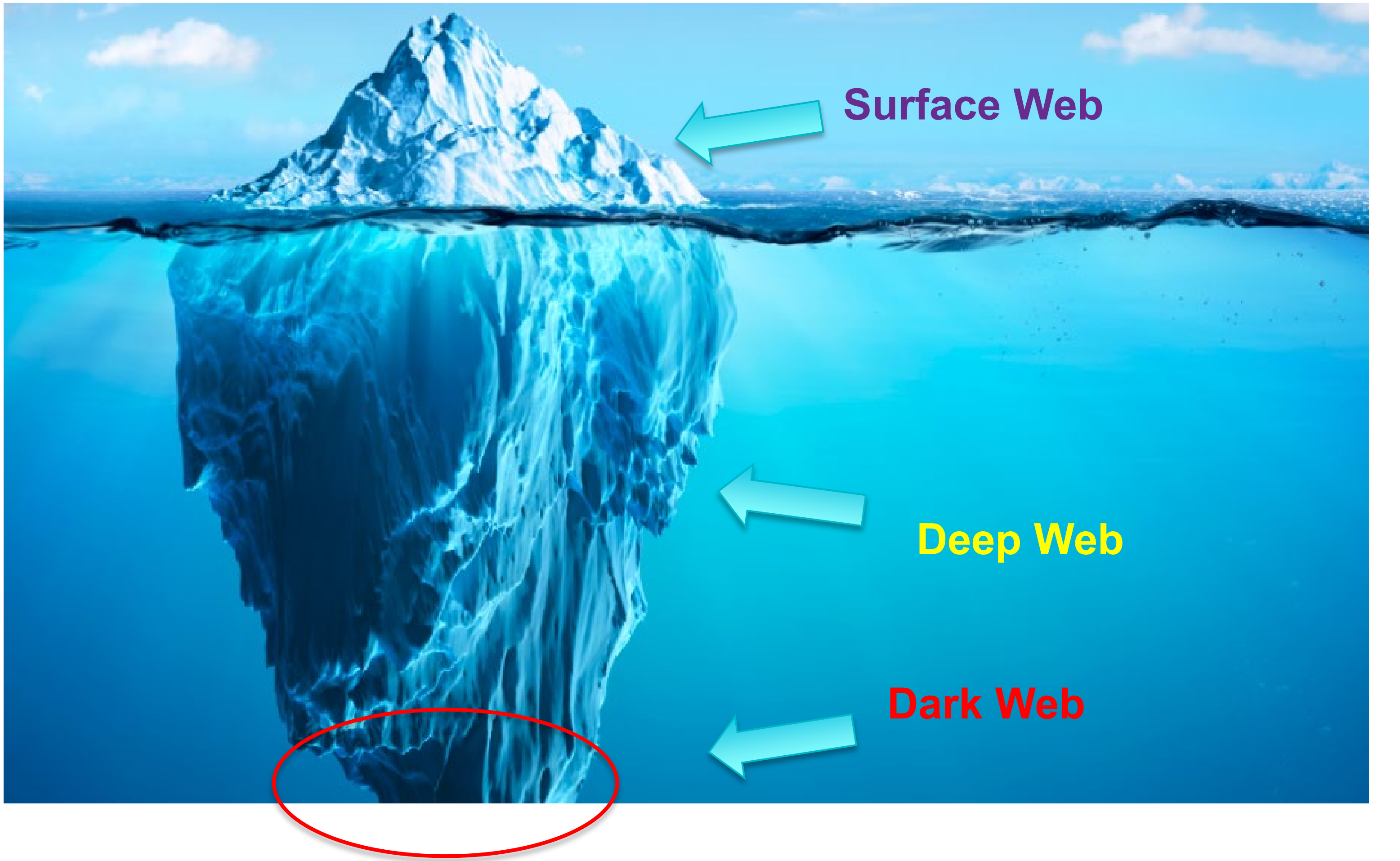
Cybercrime as an Enterprise

Cybercrime is a Commercial Business

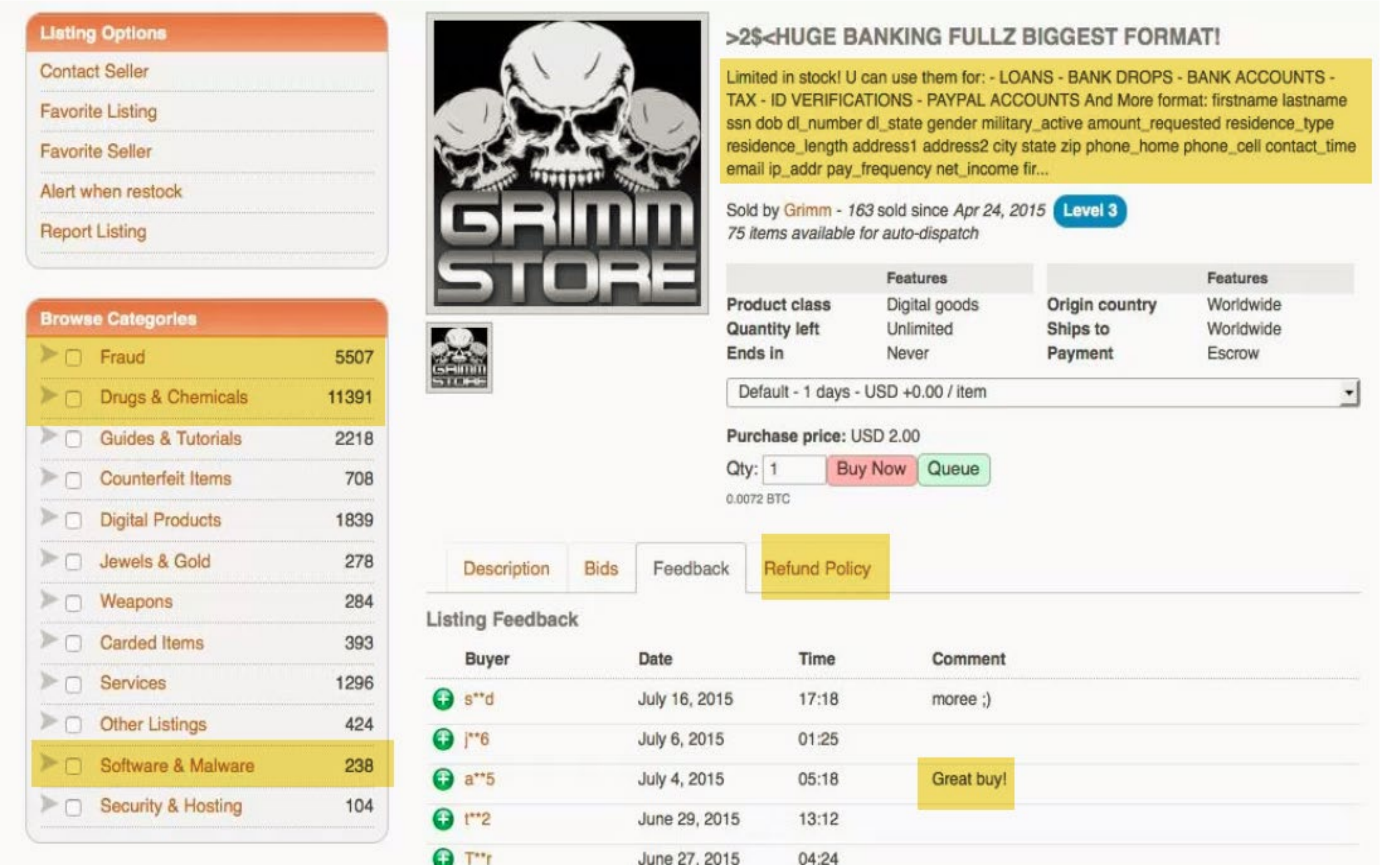
- Malware is specifically written to target bank accounts, credit card information, personal information etc.
- Hackers for hire
- Turn Key Solutions
  - Fraud As A Service (FAAS)
  - Attacks As A Service (AAAS)
  - Malware As A Service (MAAS)
  - Ransomware As A Service (RAAS)
  - Disinformation As A Service (DAAS)

Products and Services come with warranties, feature requests, training programs and customer support.

Web Layers



Dark Web Markets



Listing Options

- Contact Seller
- Favorite Listing
- Favorite Seller
- Alert when restock
- Report Listing

Browse Categories

□ Fraud	5507
□ Drugs & Chemicals	11391
□ Guides & Tutorials	2218
□ Counterfeit Items	708
□ Digital Products	1839
□ Jewels & Gold	278
□ Weapons	284
□ Carded Items	393
□ Services	1296
□ Other Listings	424
□ Software & Malware	238
□ Security & Hosting	104

>2$<HUGE BANKING FULLZ BIGGEST FORMAT!

Limited in stock! U can use them for: - LOANS - BANK DROPS - BANK ACCOUNTS - TAX - ID VERIFICATIONS - PAYPAL ACCOUNTS And More format: firstname lastname ssn dob dl_number dl_state gender military_active amount_requested residence_type residence_length address1 address2 city state zip phone_home phone_cell contact_time email ip_addr pay_frequency net_income fir...

Sold by Grimm - *163 sold since Apr 24, 2015* Level 3
75 items available for auto-dispatch

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 2.00

Qty: 1 Buy Now Queue

0.0072 BTC

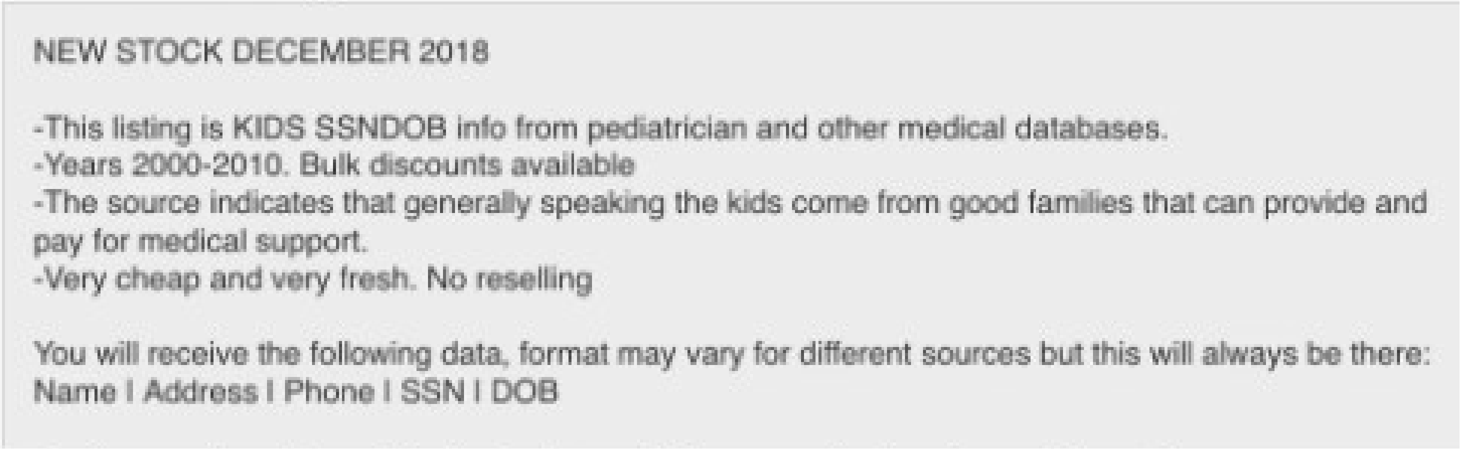
Description | Bids | Feedback | Refund Policy

Listing Feedback

Buyer	Date	Time	Comment
s**d	July 16, 2015	17:18	moree ;)
j**6	July 6, 2015	01:25	
a**5	July 4, 2015	05:18	Great buy!
t**2	June 29, 2015	13:12	
T**r	June 27, 2015	04:24	

Dark Web Markets

USA KIDS FULLZ
★ALL STATES
★ALL AGES
★1900-2010
US ONLY
SKYSCRAPER

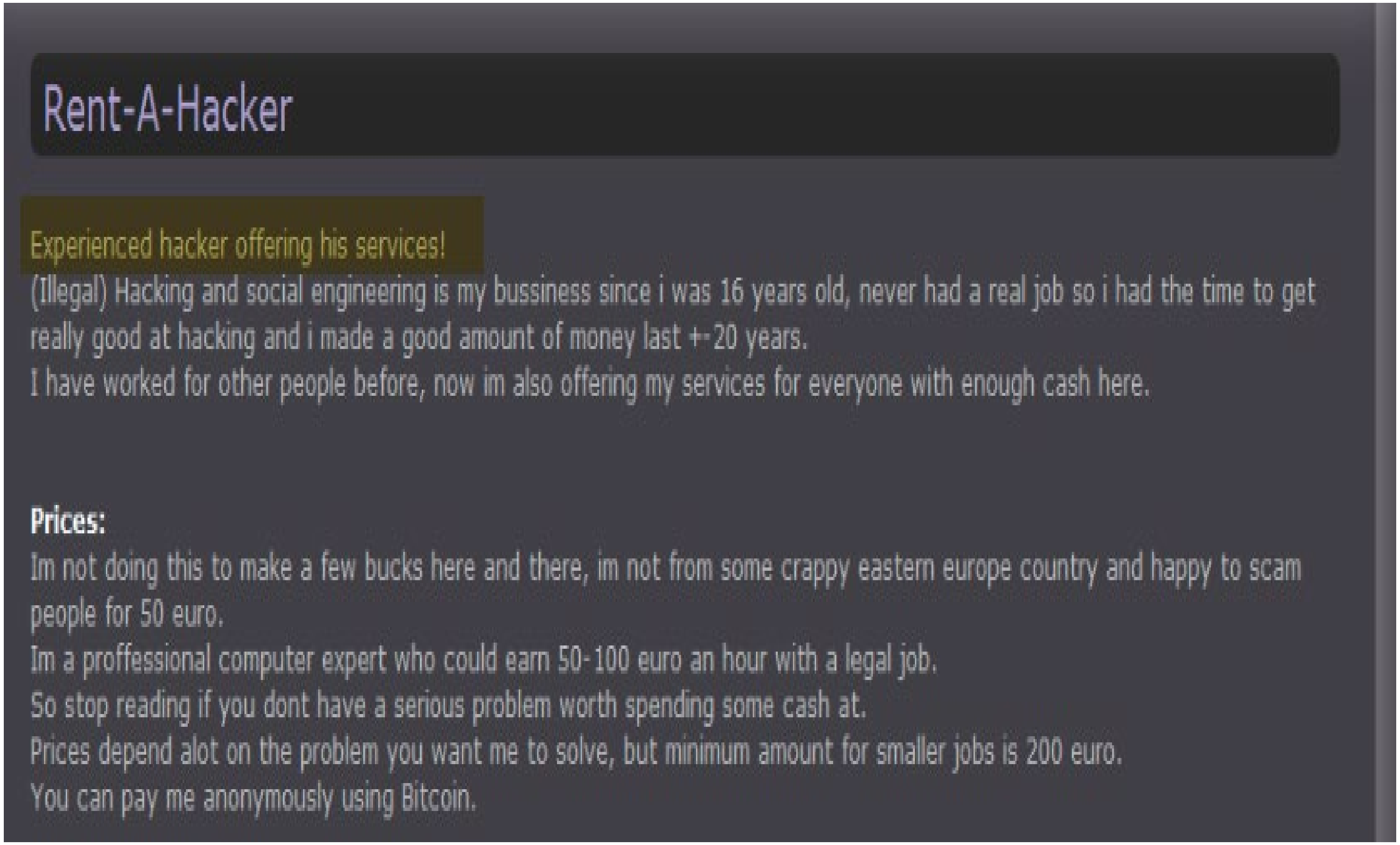


NEW STOCK DECEMBER 2018

-This listing is KIDS SSNDOB info from pediatrician and other medical databases.
-Years 2000-2010. Bulk discounts available
-The source indicates that generally speaking the kids come from good families that can provide and pay for medical support.
-Very cheap and very fresh. No reselling

You will receive the following data, format may vary for different sources but this will always be there:
Name I Address I Phone I SSN I DOB

Dark Web Markets



Rent-A-Hacker

Experienced hacker offering his services!

(Illegal) Hacking and social engineering is my bussiness since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last +-20 years.

I have worked for other people before, now im also offering my services for everyone with enough cash here.

Prices:

Im not doing this to make a few bucks here and there, im not from some crappy eastern europe country and happy to scam people for 50 euro.

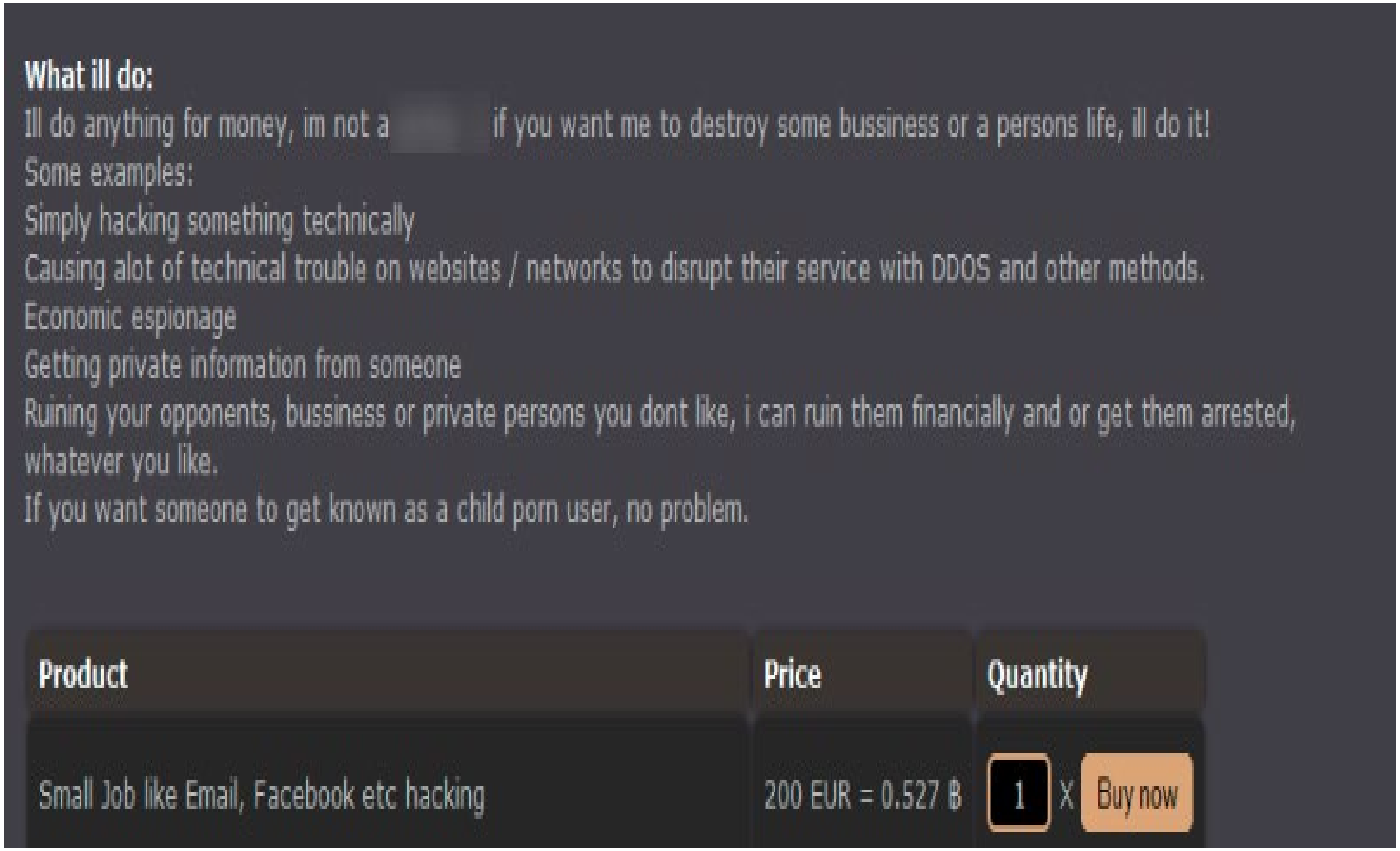
Im a proffessional computer expert who could earn 50-100 euro an hour with a legal job.

So stop reading if you dont have a serious problem worth spending some cash at.

Prices depend alot on the problem you want me to solve, but minimum amount for smaller jobs is 200 euro.

You can pay me anonymously using Bitcoin.

Dark Web Markets



What ill do:

Ill do anything for money, im not a [redacted] if you want me to destroy some bussiness or a persons life, ill do it!

Some examples:

Simply hacking something technically

Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.

Economic espionage

Getting private information from someone

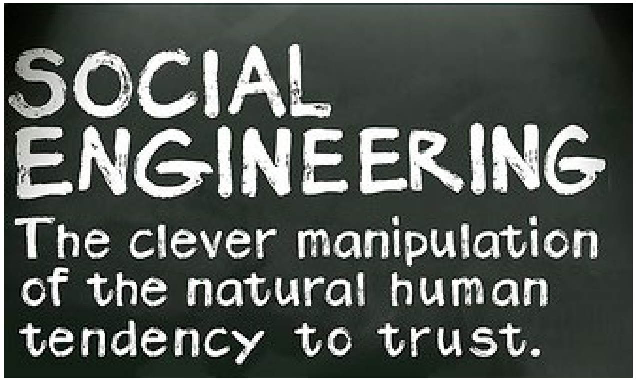
Ruining your opponents, bussiness or private persons you dont like, i can ruin them financially and or get them arrested, whatever you like.

If you want someone to get known as a child porn user, no problem.

Product	Price	Quantity
Small Job like Email, Facebook etc hacking	200 EUR = 0.527 ฿	1 X Buy now

Social Engineering

- Social engineering is the act of manipulating people into performing actions or divulging confidential information by way of social interaction
  - *voice, e-mail, social media, etc.*



SOCIAL ENGINEERING

The clever manipulation of the natural human tendency to trust.

Social Engineering – Common Elements

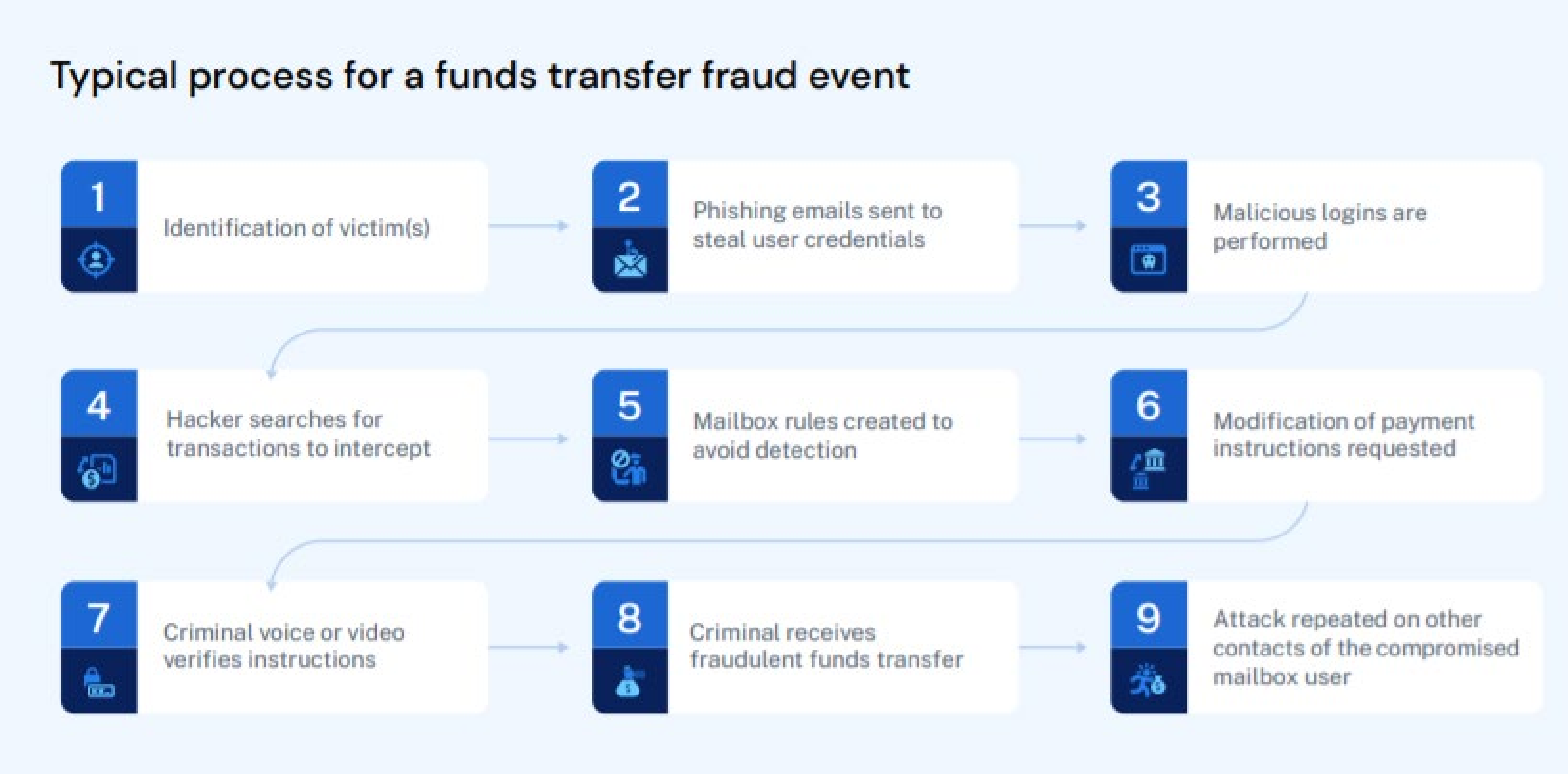
- Most Social Engineering attempts have common elements.
- They try to:
  - Elicit an emotional response
    - Fear
    - Anger
    - Curiosity
    - Sadness
- They have a sense of urgency for a task to be completed.
- They leverage world or regional events (Covid, Israel)

Social Engineering

- Phishing
- Smishing
- Vishing
- Quishing

Business E-Mail Compromise

- Pretexting

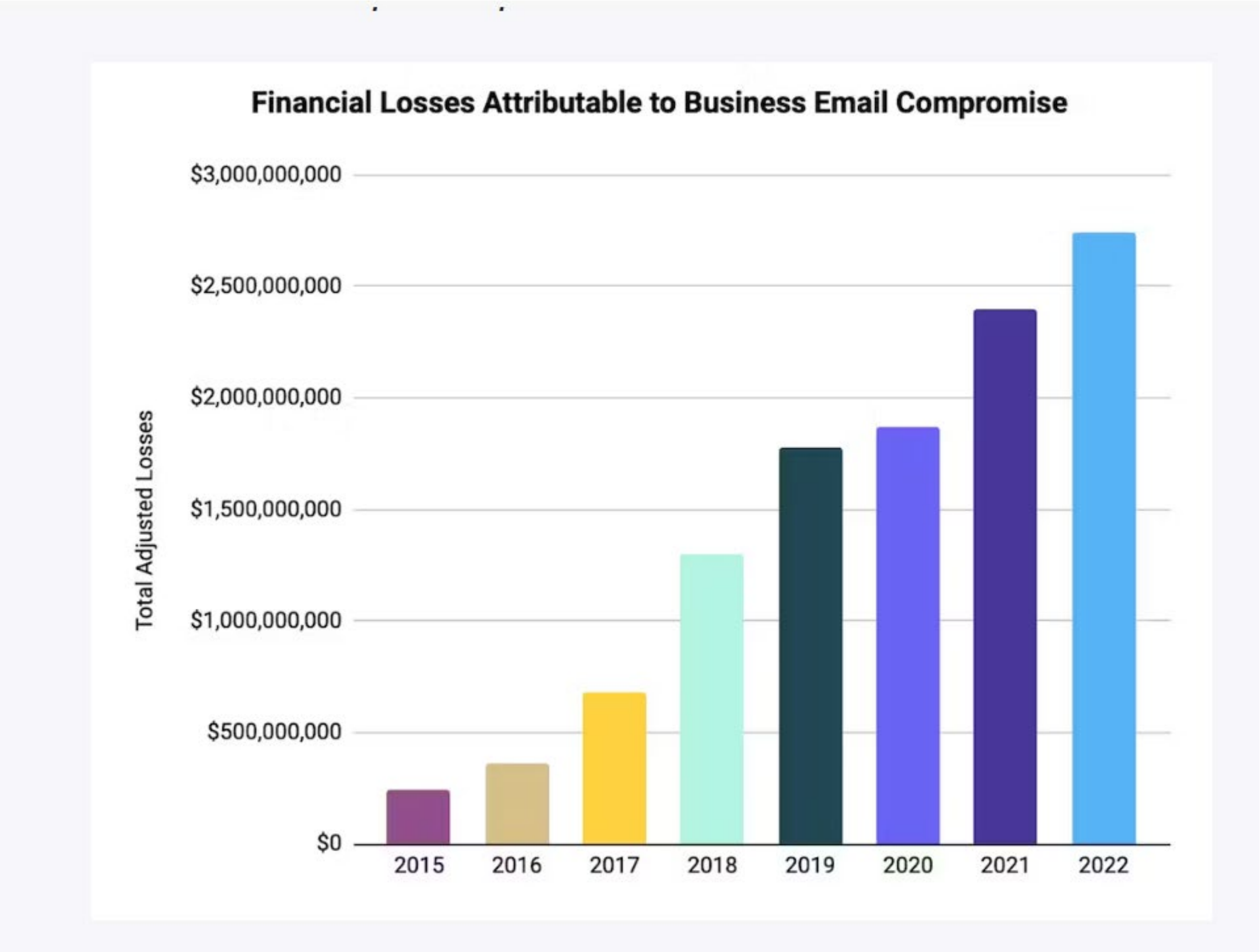


Typical process for a funds transfer fraud event

1. Identification of victim(s)
2. Phishing emails sent to steal user credentials
3. Malicious logins are performed
4. Hacker searches for transactions to intercept
5. Mailbox rules created to avoid detection
6. Modification of payment instructions requested
7. Criminal voice or video verifies instructions
8. Criminal receives fraudulent funds transfer
9. Attack repeated on other contacts of the compromised mailbox user

Source: Coalition

Business E-Mail Compromise

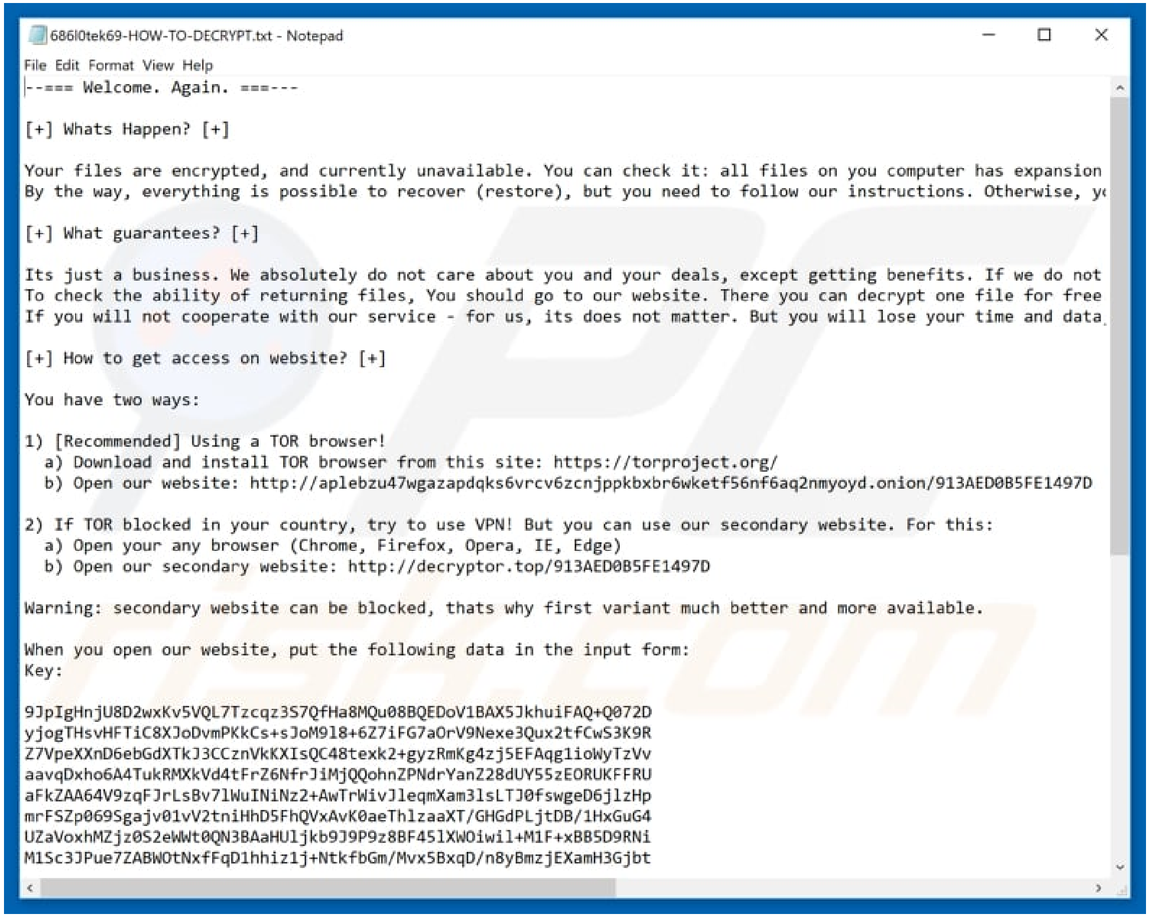


Source: Coalition

Ransomware

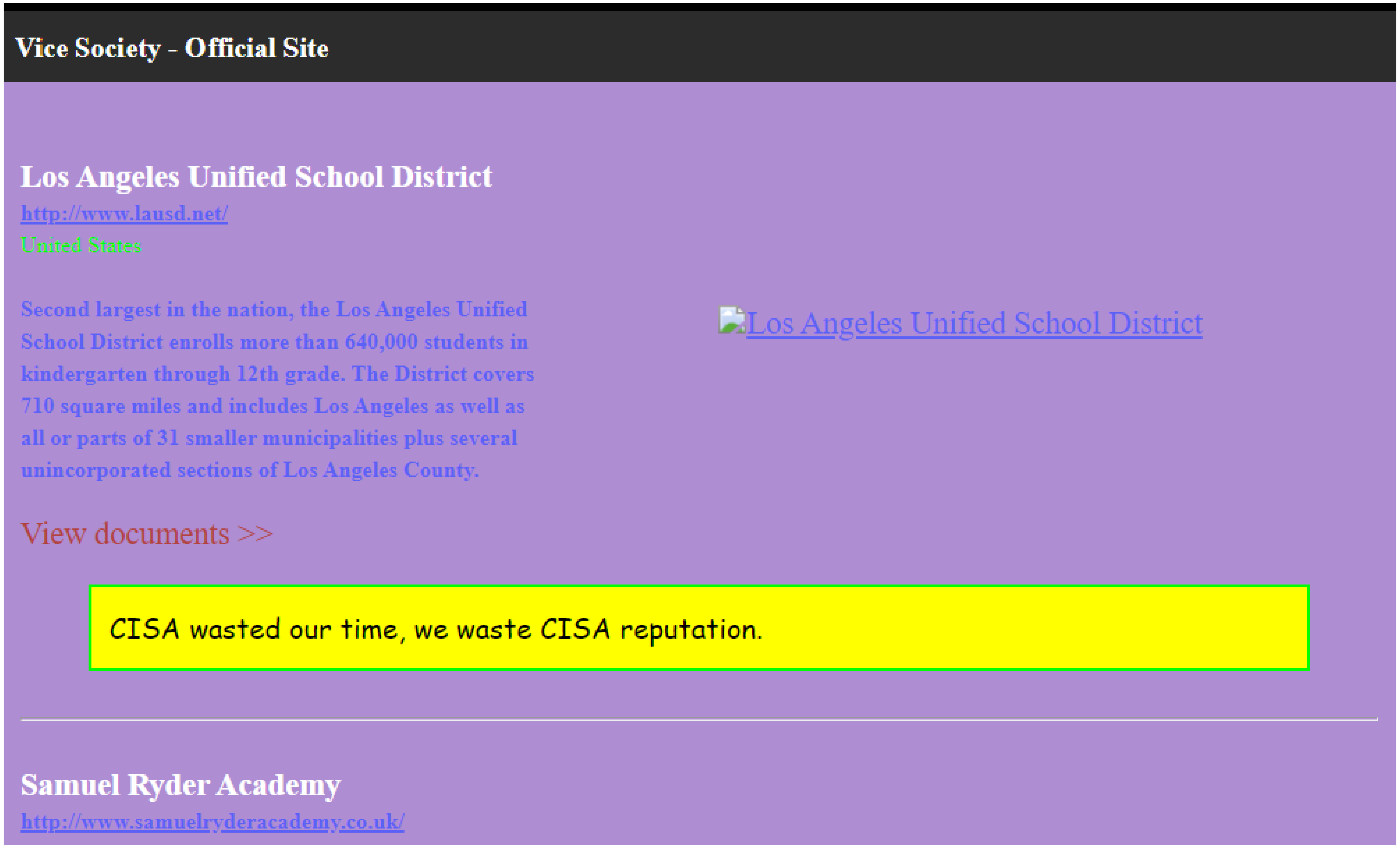
- Cyber Extortion has become one of the biggest and greatest threats to businesses and individuals.
- Ransomware = Cyber extortion
- Ransomware may be designed to:
  - Encrypt all data or systems on the network it can reach.
  - Take down systems by way of denial-of-service attacks.
  - Threaten to expose sensitive information – Social Security Numbers, Credit Card Numbers, etc.

Ransomware


686l0tek69-HOW-TO-DECRYPT.txt - Notepad
File Edit Format View Help

```
--=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, y

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not
To check the ability of returning files, You should go to our website. There you can decrypt one file for free
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/913AED0B5FE1497D

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.top/913AED0B5FE1497D

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

9JpIgHnjU8D2wxKv5VQL7Tzcqz3S7QfHa8MQu08BQEDoV1BAX5JkhuiFAQ+Q072D
yjogTHsvHFTiC8XJoDvmPKkCs+sJoM918+6Z7iFG7aOrV9Nexe3Qux2tfCwS3K9R
Z7VpeXXnD6ebGdXTkJ3CCznVkKXIsQC48texk2+gyzRmKg4zj5EFAqg1ioWyTzVv
aavqDxho6A4TukRMXkVd4tFrZ6NfrJiMjQQohnZPNdrYanZ28dUY55zEORUKFFRU
aFkZAA64V9zqFJrLsBv7lWuINiNz2+AwTrWivJleqmXam3lsLTJ0fswgeD6jlzHp
mrFSZp069Sgajv01vV2tniHhD5FhQVxAvK0aeThlzaaXT/GHGdPLjtDB/1HxGuG4
UZaVoxhMZjz0S2eWWt0QN3BAaHUljkb9J9P9z8BF45lXWOiwil+M1F+xBB5D9RNi
M1Sc3JPue7ZABWOtNxfFqD1hhiz1j+NtkfbGm/Mvx5BxqD/n8yBmzjEXamH3Gjbt
```

Ransomware



Vice Society - Official Site

Los Angeles Unified School District

http://www.lausd.net/

United States

Second largest in the nation, the Los Angeles Unified School District enrolls more than 640,000 students in kindergarten through 12th grade. The District covers 710 square miles and includes Los Angeles as well as all or parts of 31 smaller municipalities plus several unincorporated sections of Los Angeles County.

Los Angeles Unified School District

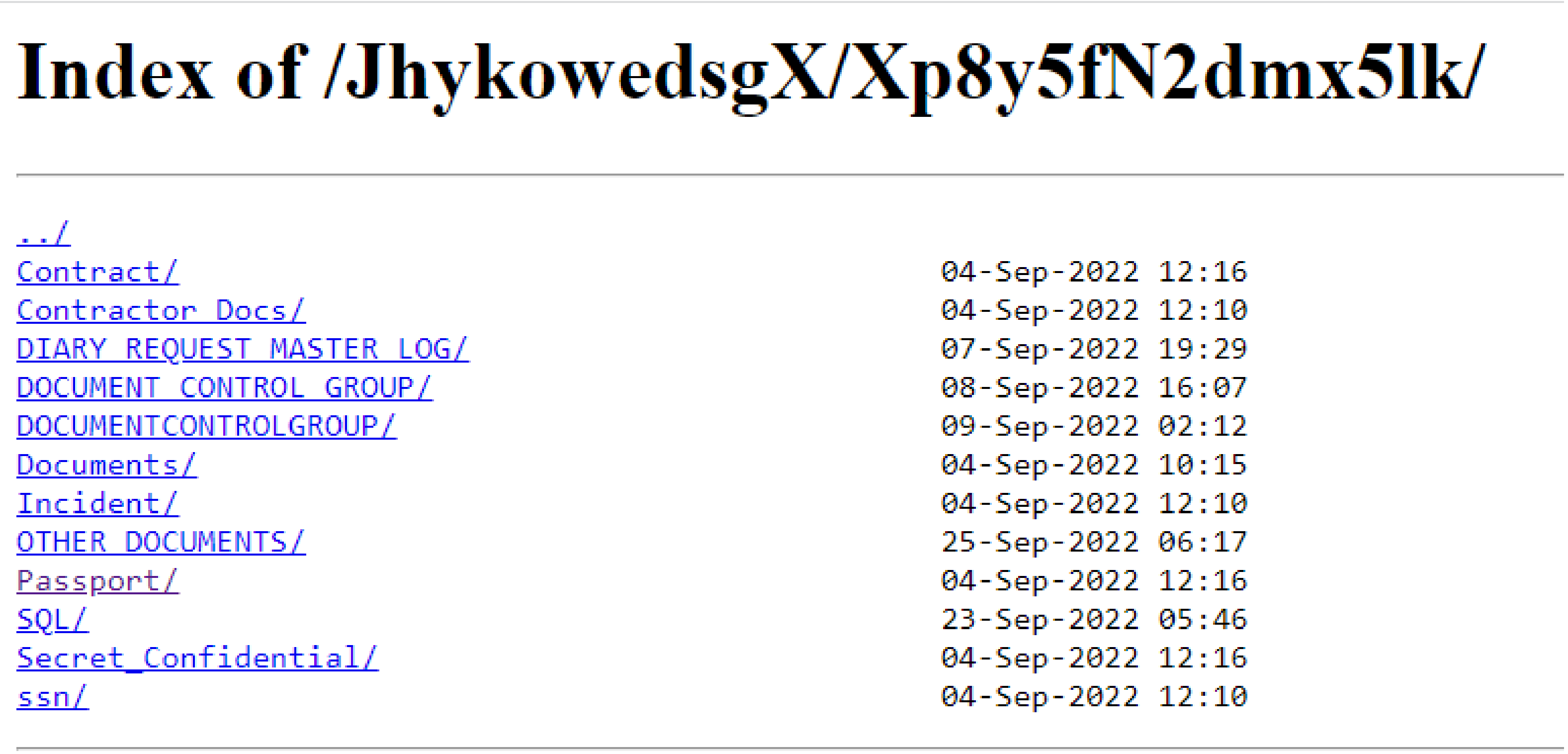
View documents >>

CISA wasted our time, we waste CISA reputation.

Samuel Ryder Academy

http://www.samuelryderacademy.co.uk/

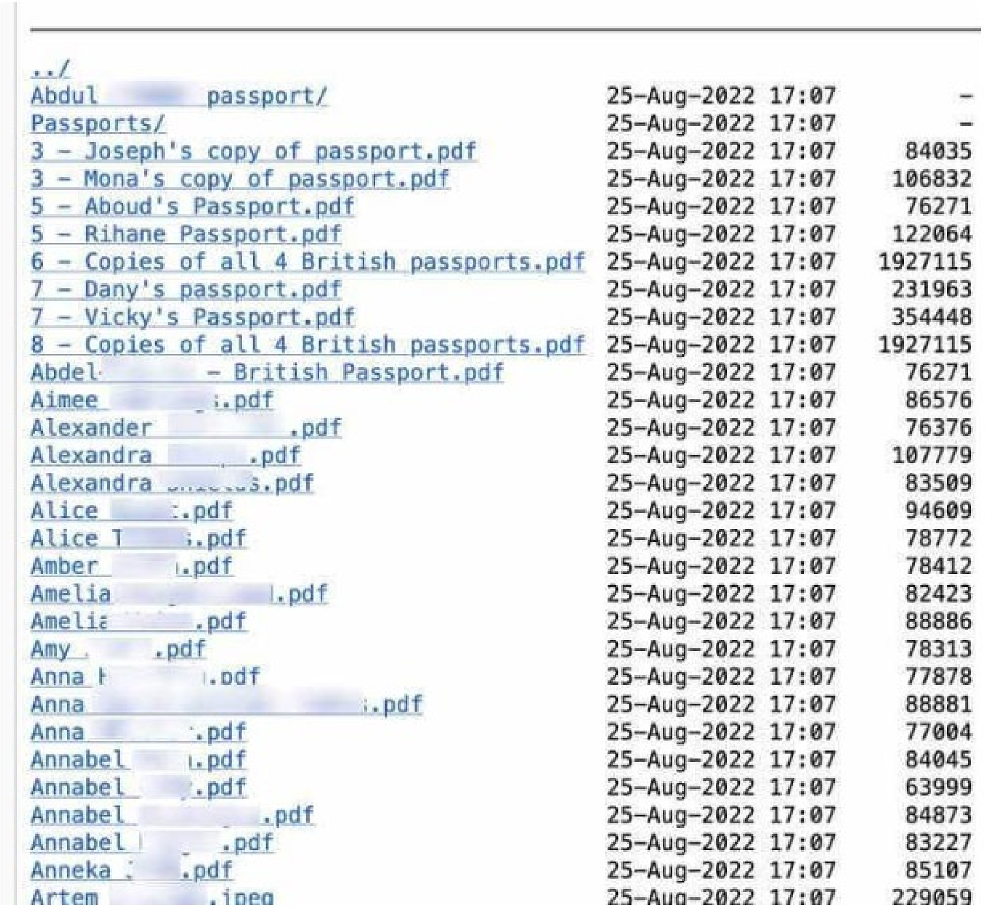
Ransomware



Index of /JhykowedsgX/Xp8y5fN2dmx5lk/

```
../
Contract/                                         04-Sep-2022 12:16
Contractor Docs/                                  04-Sep-2022 12:10
DIARY REQUEST MASTER LOG/                         07-Sep-2022 19:29
DOCUMENT CONTROL GROUP/                           08-Sep-2022 16:07
DOCUMENTCONTROLGROUP/                             09-Sep-2022 02:12
Documents/                                        04-Sep-2022 10:15
Incident/                                         04-Sep-2022 12:10
OTHER DOCUMENTS/                                  25-Sep-2022 06:17
Passport/                                         04-Sep-2022 12:16
SQL/                                              23-Sep-2022 05:46
Secret_Confidential/                              04-Sep-2022 12:16
ssn/                                              04-Sep-2022 12:10
```

Ransomware



```
../
Abdul [redacted] passport/                     25-Aug-2022 17:07          -
Passports/                                     25-Aug-2022 17:07          -
3 - Joseph's copy of passport.pdf              25-Aug-2022 17:07      84035
3 - Mona's copy of passport.pdf                25-Aug-2022 17:07     106832
5 - Aboud's Passport.pdf                       25-Aug-2022 17:07      76271
5 - Rihane Passport.pdf                        25-Aug-2022 17:07     122064
6 - Copies of all 4 British passports.pdf      25-Aug-2022 17:07    1927115
7 - Dany's passport.pdf                        25-Aug-2022 17:07     231963
7 - Vicky's Passport.pdf                       25-Aug-2022 17:07     354448
8 - Copies of all 4 British passports.pdf      25-Aug-2022 17:07    1927115
Abdel [redacted] - British Passport.pdf        25-Aug-2022 17:07      76271
Aimee [redacted].pdf                           25-Aug-2022 17:07      86576
Alexander [redacted].pdf                       25-Aug-2022 17:07      76376
Alexandra [redacted].pdf                       25-Aug-2022 17:07     107779
Alexandra [redacted].pdf                       25-Aug-2022 17:07      83509
Alice [redacted].pdf                           25-Aug-2022 17:07      94609
Alice [redacted].pdf                           25-Aug-2022 17:07      78772
Amber [redacted].pdf                           25-Aug-2022 17:07      78412
Amelia [redacted].pdf                          25-Aug-2022 17:07      82423
Amelia [redacted].pdf                          25-Aug-2022 17:07      88886
Amy [redacted].pdf                             25-Aug-2022 17:07      78313
Anna [redacted].pdf                            25-Aug-2022 17:07      77878
Anna [redacted].pdf                            25-Aug-2022 17:07      88881
Anna [redacted].pdf                            25-Aug-2022 17:07      77004
Annabel [redacted].pdf                         25-Aug-2022 17:07      84045
Annabel [redacted].pdf                         25-Aug-2022 17:07      63999
Annabel [redacted].pdf                         25-Aug-2022 17:07      84873
Annabel [redacted].pdf                         25-Aug-2022 17:07      83227
Anneka [redacted].pdf                          25-Aug-2022 17:07      85107
Artem [redacted].jpeg                          25-Aug-2022 17:07     229059
```

Third Party Risk

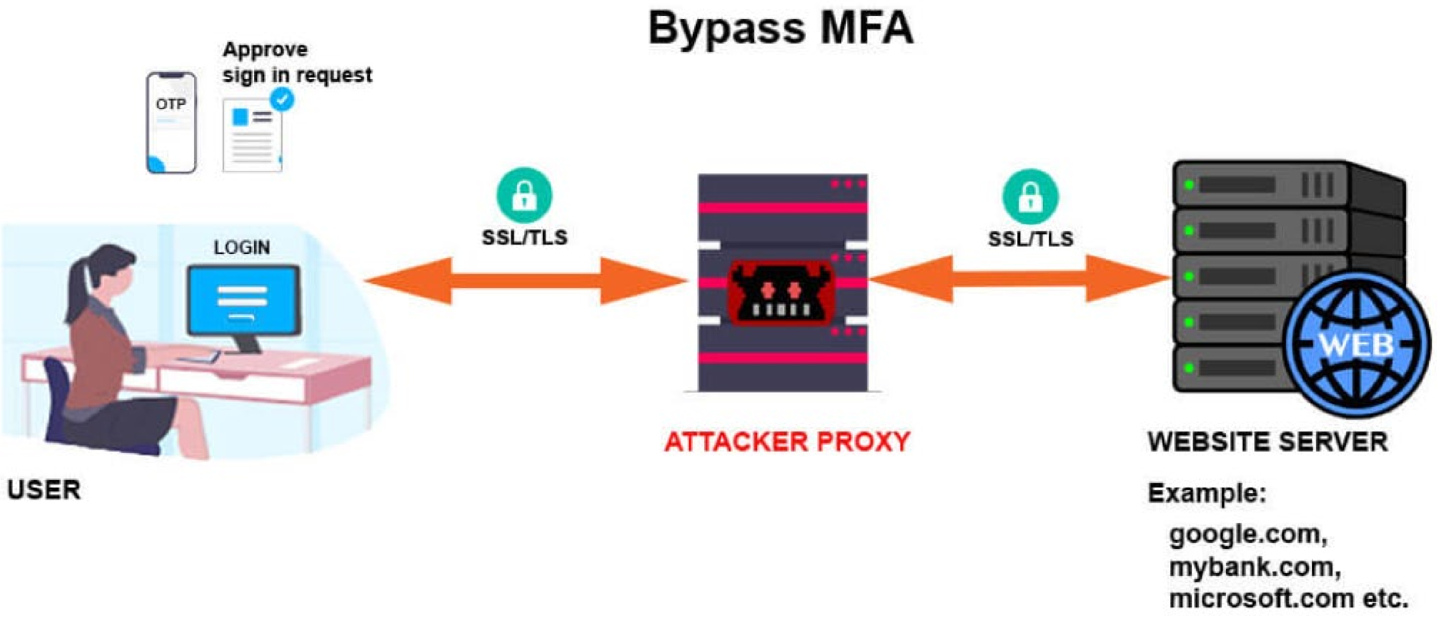
- 53% of companies have experienced a data breach related to third parties in the past year (Ponemon Institute).
- Notable Third-Party Incidents:
  - TJMax
  - Solarwinds
  - MOVEit

Attack Evolution

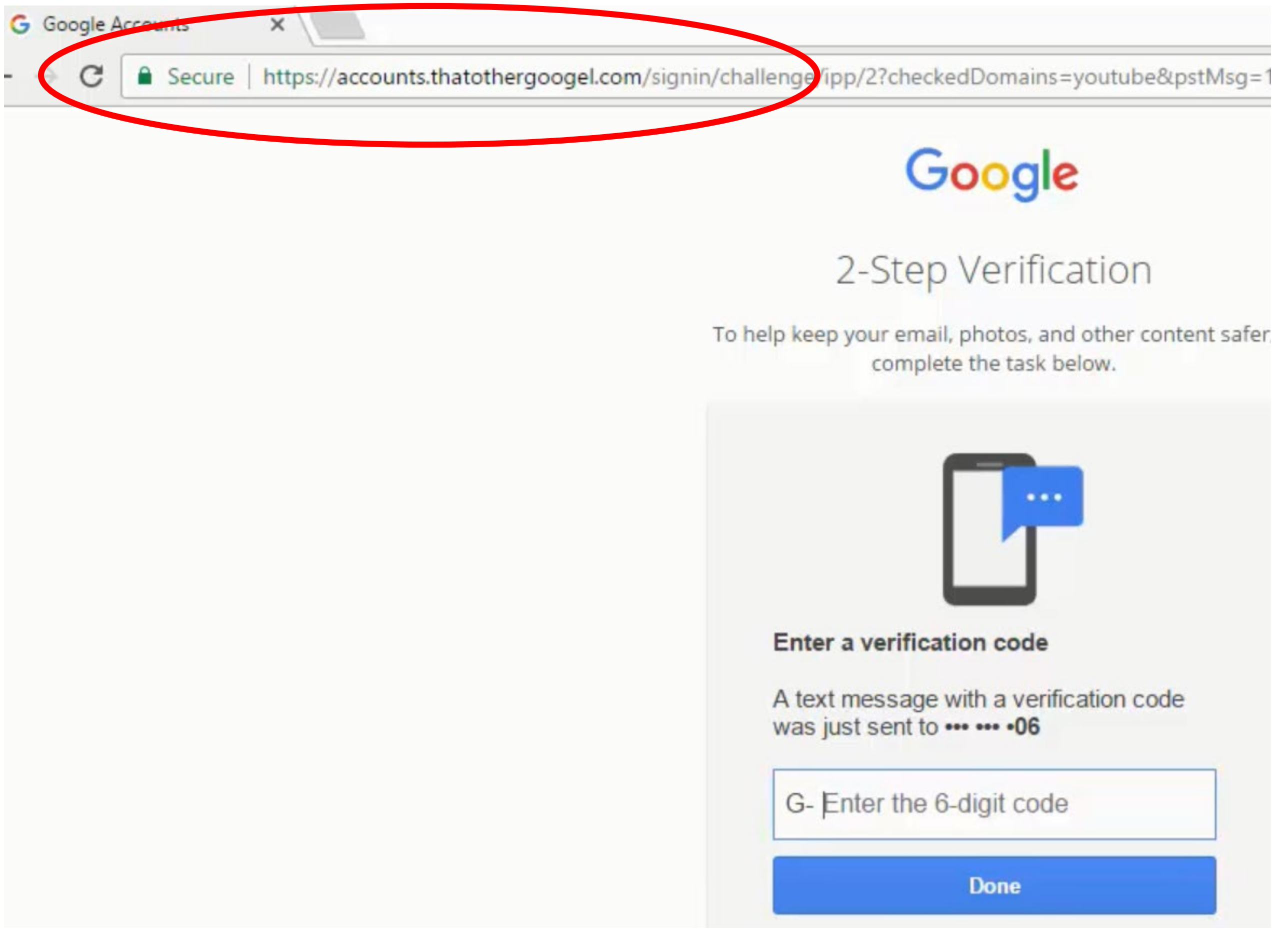
MFA Bypass

- MFA is being actively and consistently bypassed
- Tactics used:
  - MFA Fatigue
  - SIM Swap
  - Session Hijacking

MFA Bypass


Bypass MFA
OTP
Approve
sign in request
LOGIN
USER
SSL/TLS
SSL/TLS
ATTACKER PROXY
WEB
WEBSITE SERVER
Example:
google.com,
mybank.com,
microsoft.com etc.

MFA Bypass



https://accounts.thatothergoogel.com/signin/challenge/ipp/2?checkedDomains=youtube&pstMsg=1

2-Step Verification

To help keep your email, photos, and other content safer complete the task below.

Enter a verification code

A text message with a verification code was just sent to ••• ••• •06

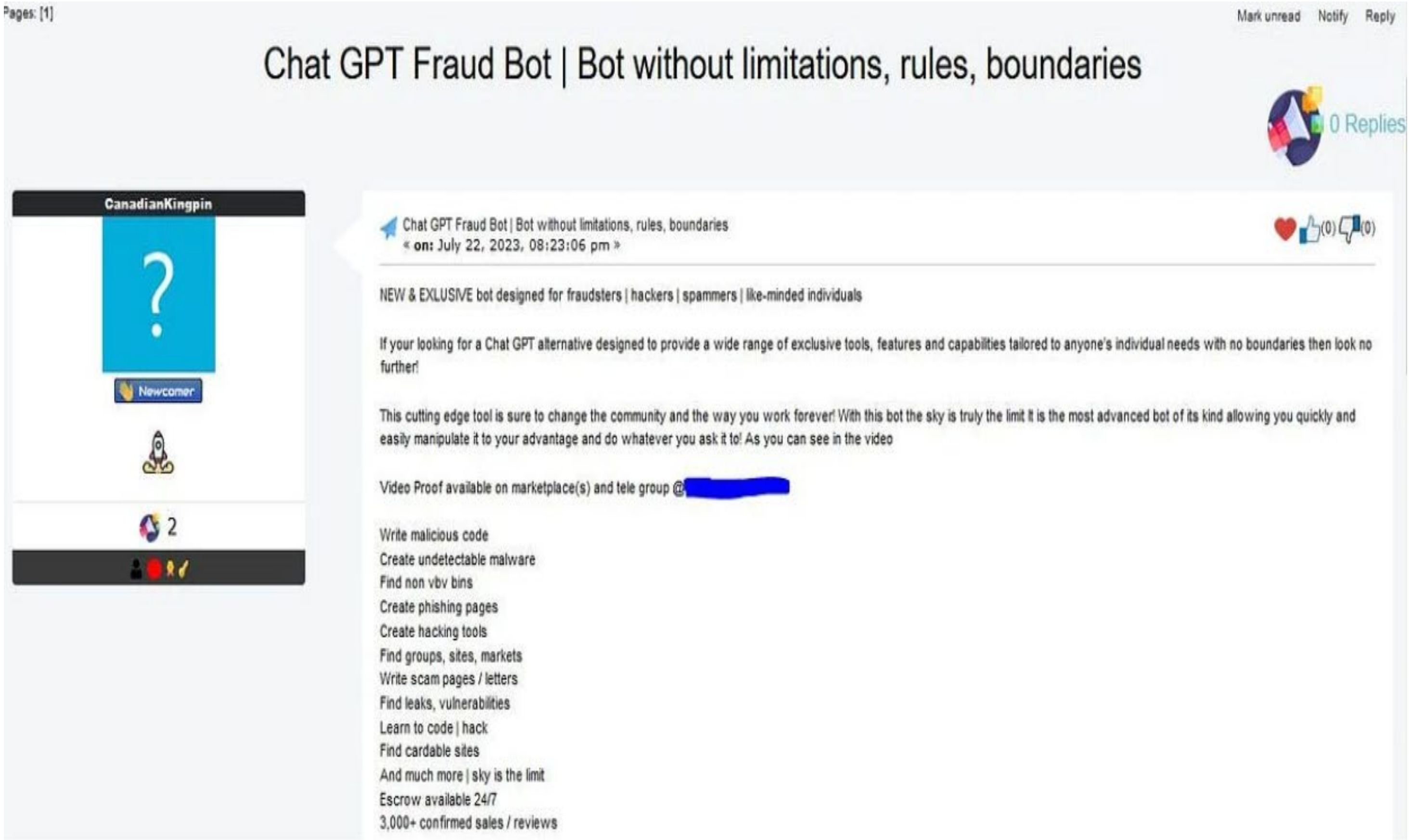
G- Enter the 6-digit code

Artificial Intelligence

- Will be leveraged heavily in attack generation
  - Specifically in social engineering

- Will be critical to defend against modern attacks.
  - Computer vs. Computer

Dark Web Markets



Pages: [1]

Mark unread Notify Reply

Chat GPT Fraud Bot | Bot without limitations, rules, boundaries

0 Replies

CanadianKingpin

Newcomer

2

Chat GPT Fraud Bot | Bot without limitations, rules, boundaries
« on: July 22, 2023, 08:23:06 pm »

(0) (0)

NEW & EXLUSIVE bot designed for fraudsters | hackers | spammers | like-minded individuals

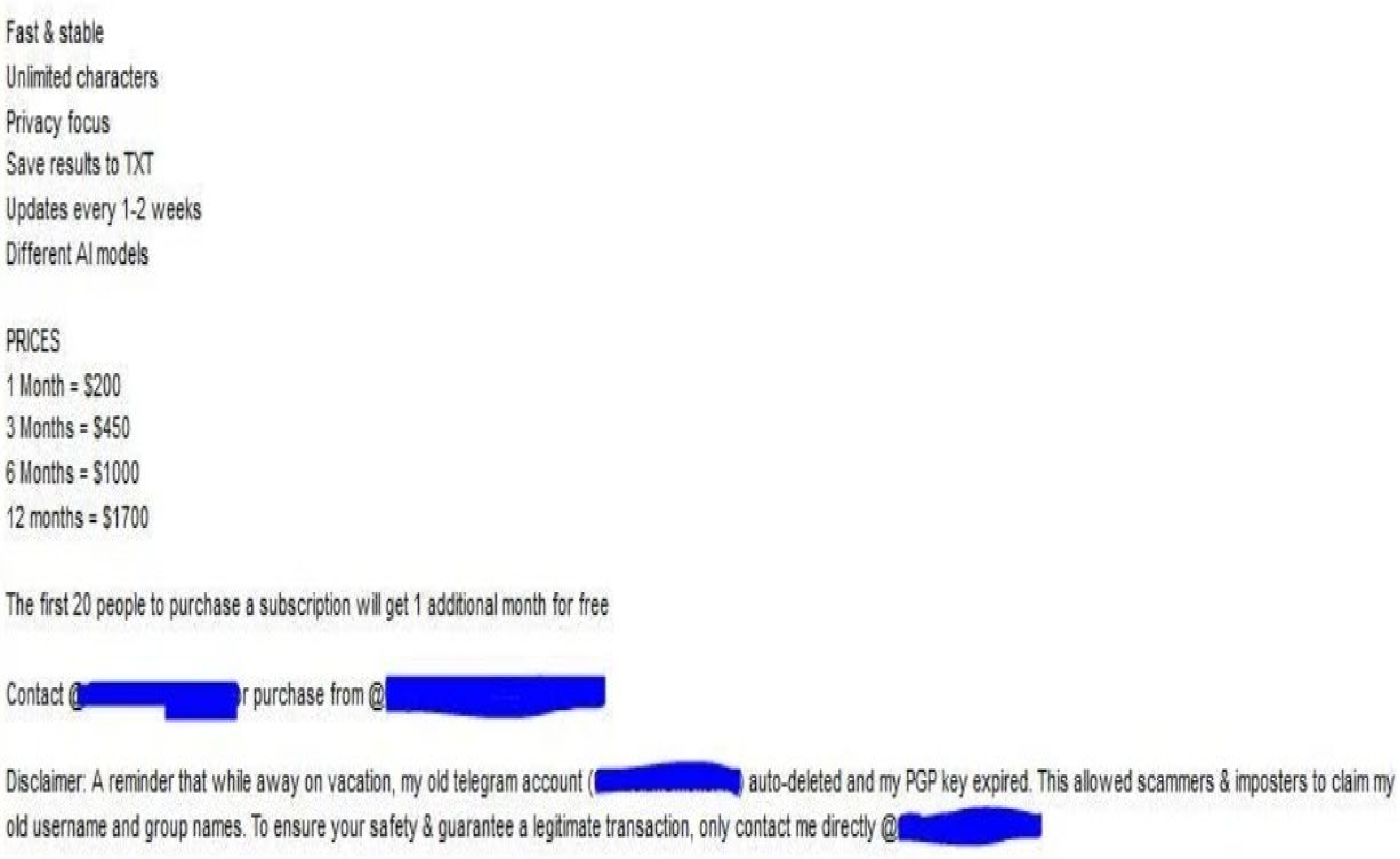
If your looking for a Chat GPT alternative designed to provide a wide range of exclusive tools, features and capabilities tailored to anyone's individual needs with no boundaries then look no further!

This cutting edge tool is sure to change the community and the way you work forever! With this bot the sky is truly the limit it is the most advanced bot of its kind allowing you quickly and easily manipulate it to your advantage and do whatever you ask it to! As you can see in the video

Video Proof available on marketplace(s) and tele group @[redacted]

Write malicious code
Create undetectable malware
Find non vbv bins
Create phishing pages
Create hacking tools
Find groups, sites, markets
Write scam pages / letters
Find leaks, vulnerabilities
Learn to code | hack
Find cardable sites
And much more | sky is the limit
Escrow available 24/7
3,000+ confirmed sales / reviews

Dark Web Markets



Fast & stable
Unlimited characters
Privacy focus
Save results to TXT
Updates every 1-2 weeks
Different AI models

PRICES
1 Month = $200
3 Months = $450
6 Months = $1000
12 months = $1700

The first 20 people to purchase a subscription will get 1 additional month for free

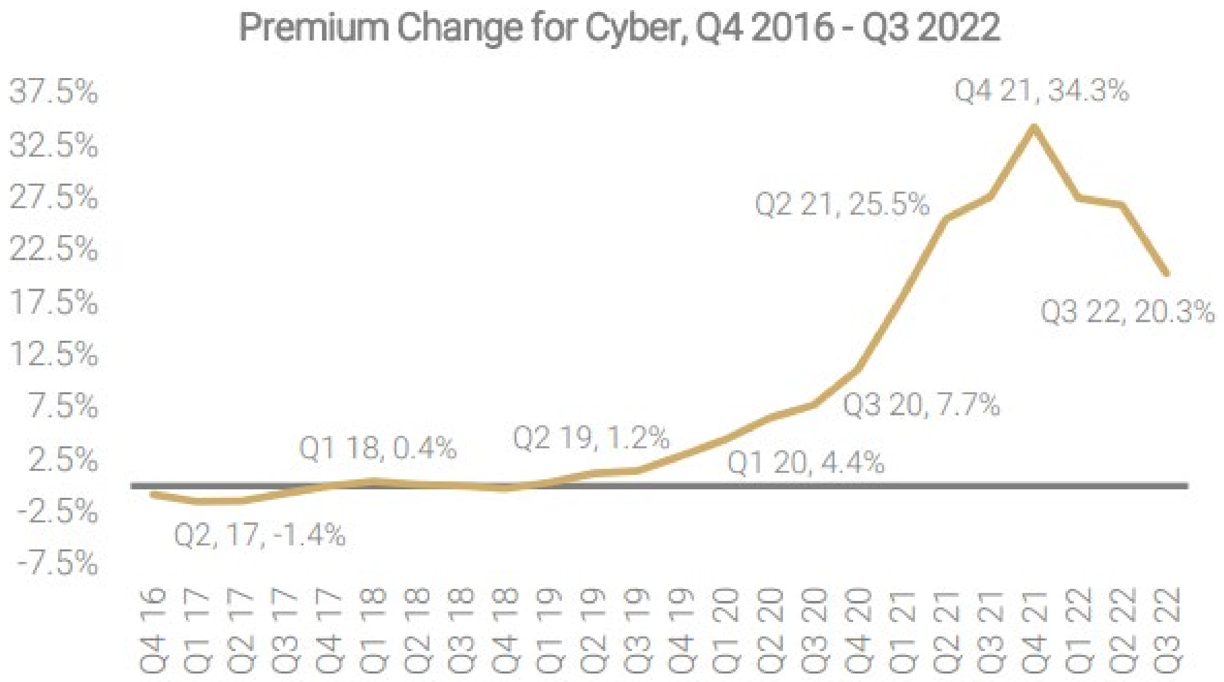
Contact @[redacted]r purchase from @[redacted]

Disclaimer: A reminder that while away on vacation, my old telegram account ([redacted]) auto-deleted and my PGP key expired. This allowed scammers & imposters to claim my old username and group names. To ensure your safety & guarantee a legitimate transaction, only contact me directly @[redacted]

Welcome to DeepFake

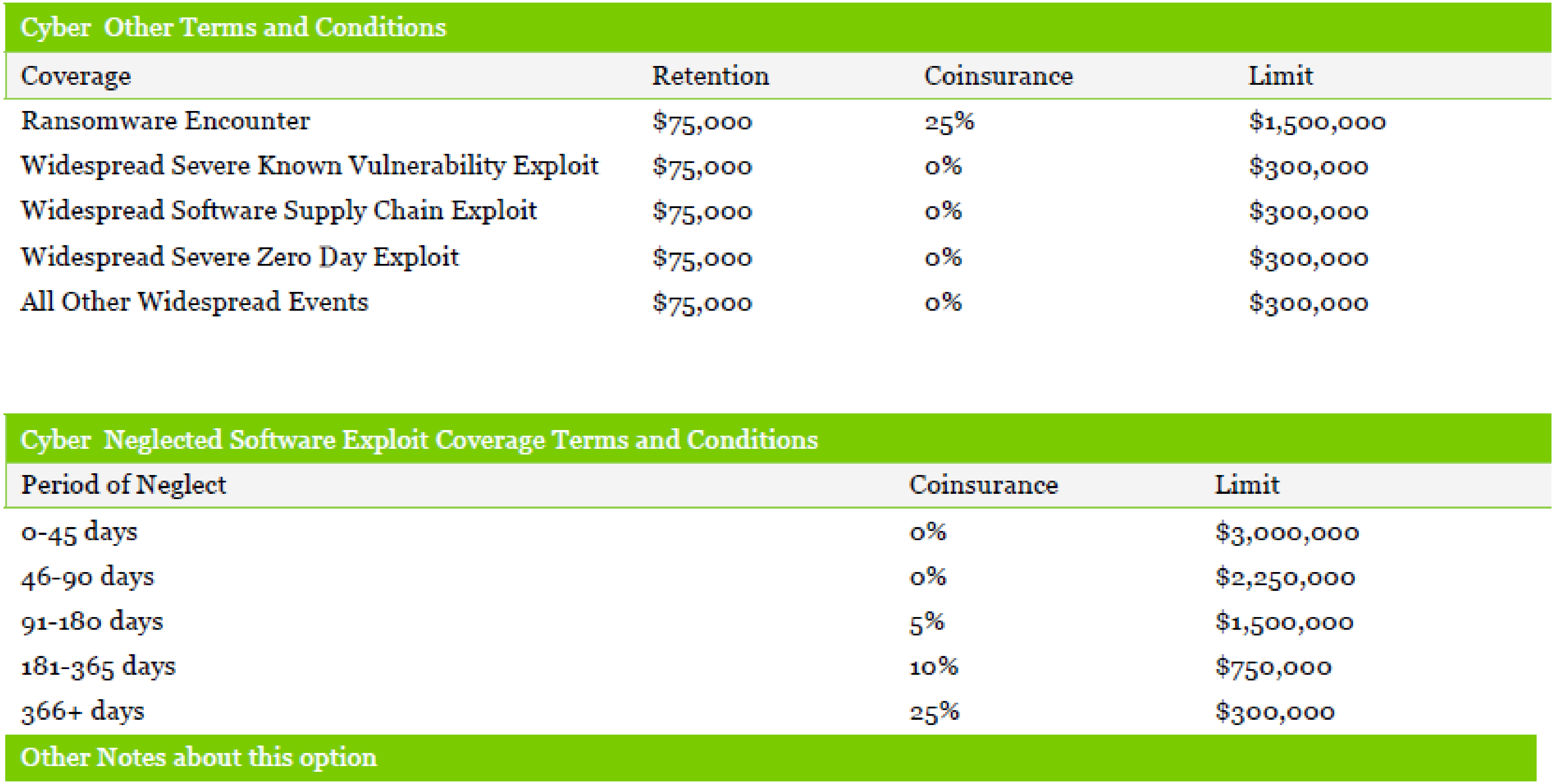
Transfer the Risk

Cyber Insurance



Source: Council of Insurance Agents & Brokers

Cyber Insurance

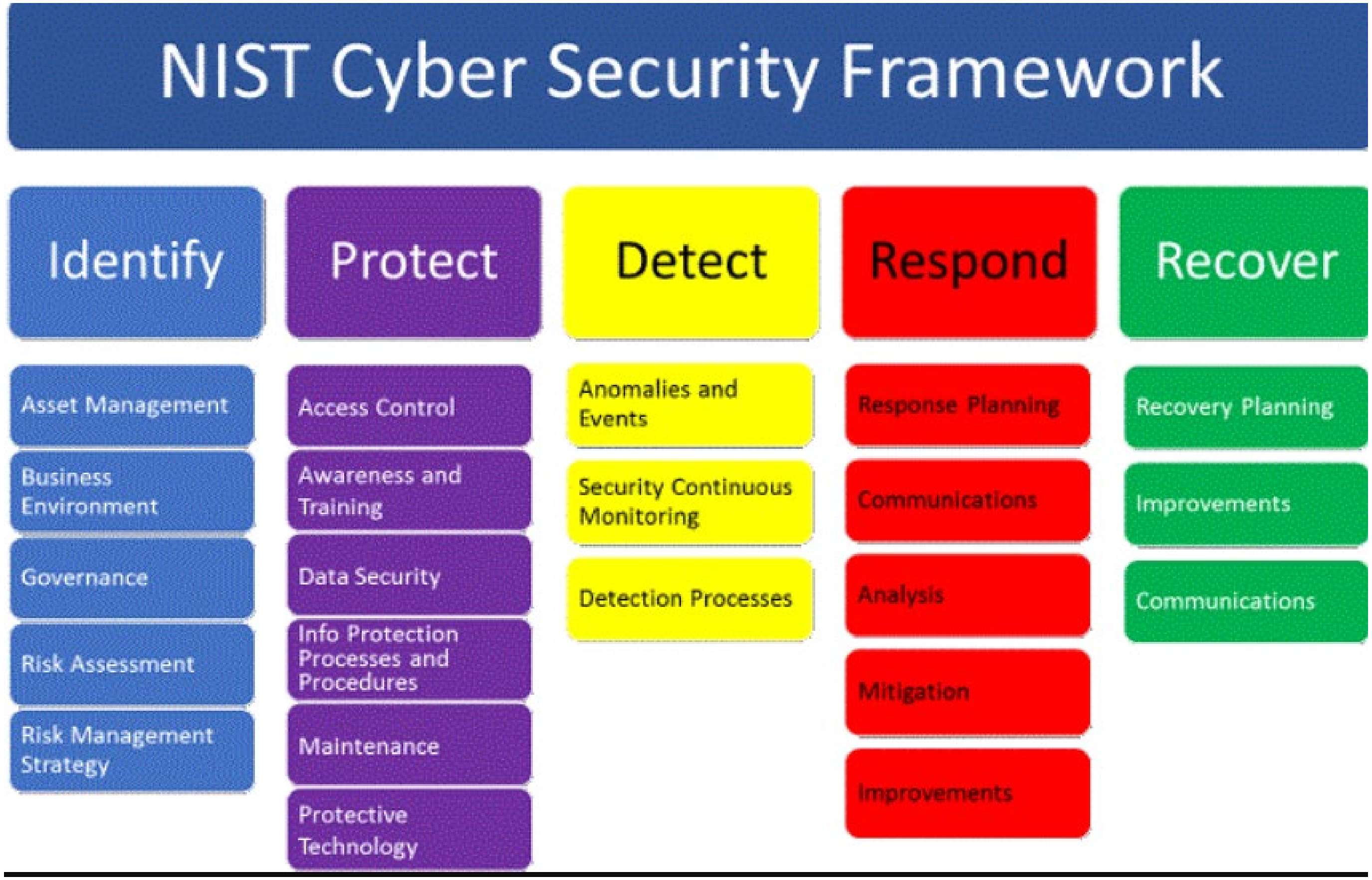


Cyber Other Terms and Conditions			
Coverage	Retention	Coinsurance	Limit
Ransomware Encounter	$75,000	25%	$1,500,000
Widespread Severe Known Vulnerability Exploit	$75,000	0%	$300,000
Widespread Software Supply Chain Exploit	$75,000	0%	$300,000
Widespread Severe Zero Day Exploit	$75,000	0%	$300,000
All Other Widespread Events	$75,000	0%	$300,000

Cyber Neglected Software Exploit Coverage Terms and Conditions		
Period of Neglect	Coinsurance	Limit
0-45 days	0%	$3,000,000
46-90 days	0%	$2,250,000
91-180 days	5%	$1,500,000
181-365 days	10%	$750,000
366+ days	25%	$300,000
Other Notes about this option		

Source: Council of Insurance Agents & Brokers

Manage the Risk



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Identify

- Board Level Oversight and Involvement
- Inventory all IT Assets
  - Hardware
  - Software
  - Data
- Value IT Assets
- Perform Risk Assessments
  - Internal
  - Third Party
  - Penetration Testing
- Inventory Third Parties
- Stay Informed

Protect

- Establish a Cybersecurity Program
- Implement Defined and Documented Policies and Standards
- Train and Test Employee Cybersecurity Awareness
- Strong Consistent Access Controls
  - Passwords
  - Multi-Factor Authentication
- Restrict Access
- Restrict Administrative Accounts
- Control and Prevent Lateral Movement
- Encrypt Data at Rest and in Transit

Protect

- Malware Detection and Prevention
- Patch Known Vulnerabilities
- Zero Trust
  - If you can’t validate the User and Device connecting to your IT Assets, BLOCK IT.

Detect

- Need a Toolset
  - SIEM
  - EDR or XDR
- Ensure Security Logs are:
  - Captured
  - Stored
  - Analyzed
- Establish Alerts
- Leverage AI

Respond and Recover

- Have a Backup and Recovery Strategy
  - Protect the Backups (Ransomware Resilient)
- Develop and Maintain
  - Business Continuity Plans
    - Recovery Point Objective (How much data can we lose)
    - Recovery Time Objective (How long can we be down)
  - Disaster Recovery Plans
  - Incident Response Plans
- Test and Test Again

Impacts to the Nonprofit Audit Process

- Lack of reliance / trust in the general IT controls

Questions?

Contact Us

Thomas DeMayo
tdemayo@pkfod.com

Alexander K. Buchholz
abuchholz@pkfod.com

"PKF O'Connor Davies" is the brand name under which PKF O'Connor Davies LLP and PKF O'Connor Davies Advisory LLC, independently owned entities, provide professional services in an alternative practice structure in accordance with applicable professional standards. PKF O'Connor Davies LLP is a licensed CPA firm that provides attest services and PKF O'Connor Davies Advisory LLC and its subsidiary entities provide tax and advisory services. PKF O'Connor Davies is a member of the PKF International Limited network of legally independent firms and does not accept any responsibility or liability for the actions or inactions on the part of any other individual member firm or firms.