PCBS The National Graduate School of Banking™

Welcome to

PCBS MASTERCLASS

Cybersecurity: Getting the Most Bang for Your Buck!

LMG™
SECURITY

February 16, 2023

Today’s Speaker

- **Sherri Davidoff**
- Founder & CEO, LMG Security
- **22 years** as a cybersecurity professional
- MIT, EE/CS & Network Security Team
- Training: PCBS, FDIC/FFIEC, ABA, IRS, Black Hat & more
- Author of ”Data Breaches”
- **New Book!**
    - **“Ransomware & Cyber Extortion”**

ACHIEVE
NOTHING™
No one hacked you today. There wasn't a single breach. It's business as usual.
FIND OUT MORE
GET A QUOTE
Ransomware
and
Cyber Extortion
New Book!

©LMG Security 2021. All rights reserved.

Thanks, PCBS!

PCBS

The National Graduate School of Banking™

“How Much Should We Spend on Cybersecurity?”

- The answer is…
- It depends!
- (You knew that was coming…)

Today’s Roadmap

1. Cybersecurity Requirements are Ramping Up
2. 4 Steps to an Effective Cybersecurity Program
3. Top Cybersecurity Controls for 2023

You said: “We want numbers!”
We listened ☺

The Costs of Insecurity are Rising…

- Cybersecurity incidents are VERY expensive

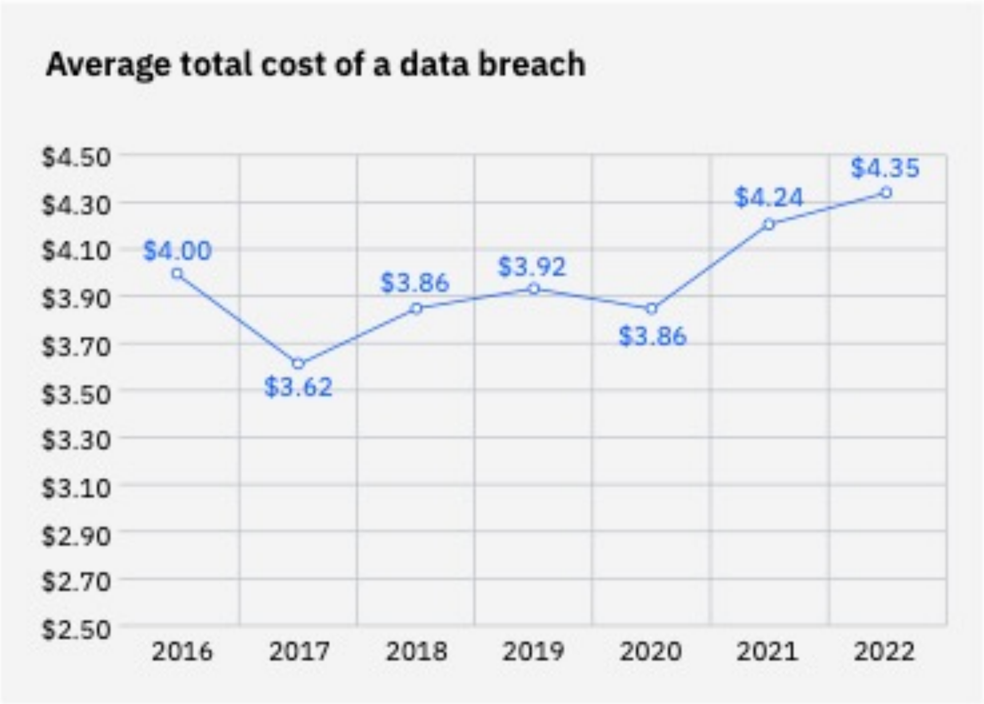


Figure 1: Measured in USD millions

USD 4.35 million

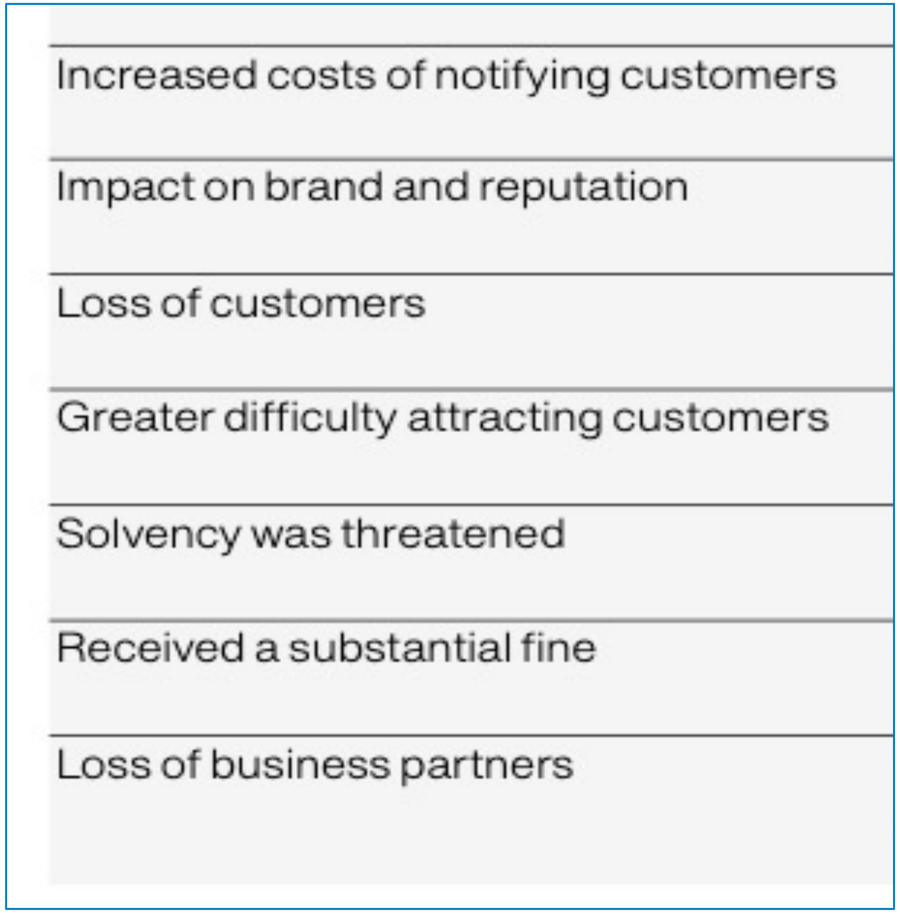
Average total cost of a data breach

USD 9.44 million

Average cost of a breach in the United States, the highest of any country

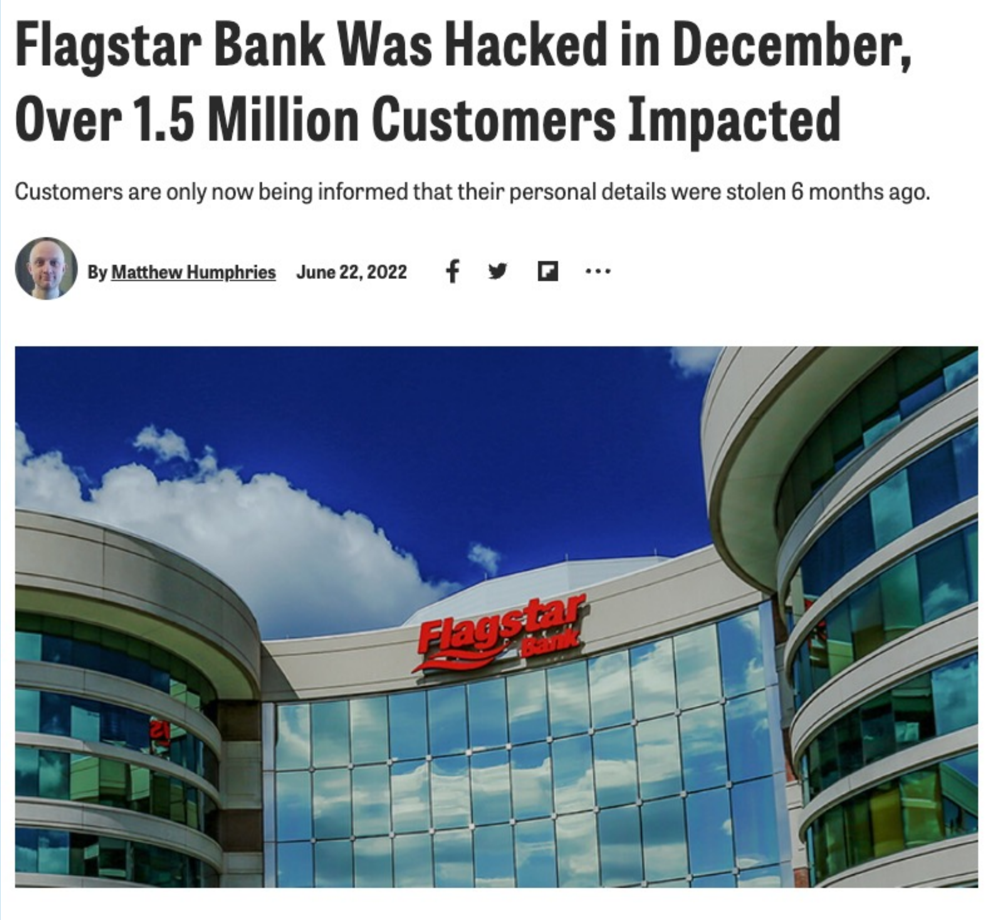
IBM.

Impacts of Cyber Attacks Go Beyond Direct Cash Loss



- Increased costs of notifying customers
- Impact on brand and reputation
- Loss of customers
- Greater difficulty attracting customers
- Solvency was threatened
- Received a substantial fine
- Loss of business partners

Hiscox, Cyber Readiness Report 2022



Flagstar Bank Was Hacked in December, Over 1.5 Million Customers Impacted

Customers are only now being informed that their personal details were stolen 6 months ago.

By Matthew Humphries June 22, 2022

©LMG Security 2021. All rights reserved. | www.LMGsecurity.com

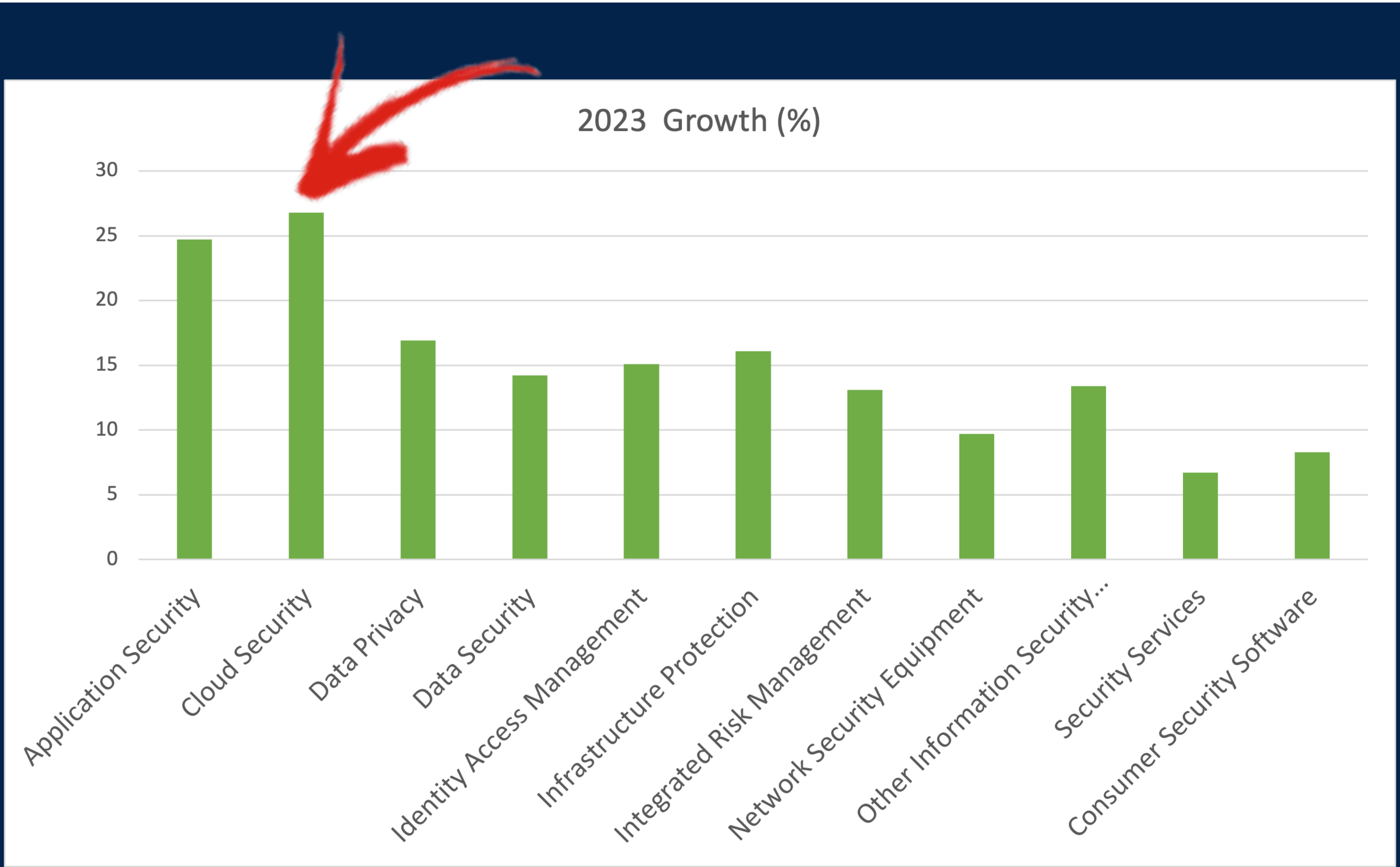
Pressure to Ramp Up Cybersecurity Programs

- Reduce risk of harm
- Regulator / examiner requirements
- Meet cyber insurer recommendations
- Customer demands
- Our communities
- & more

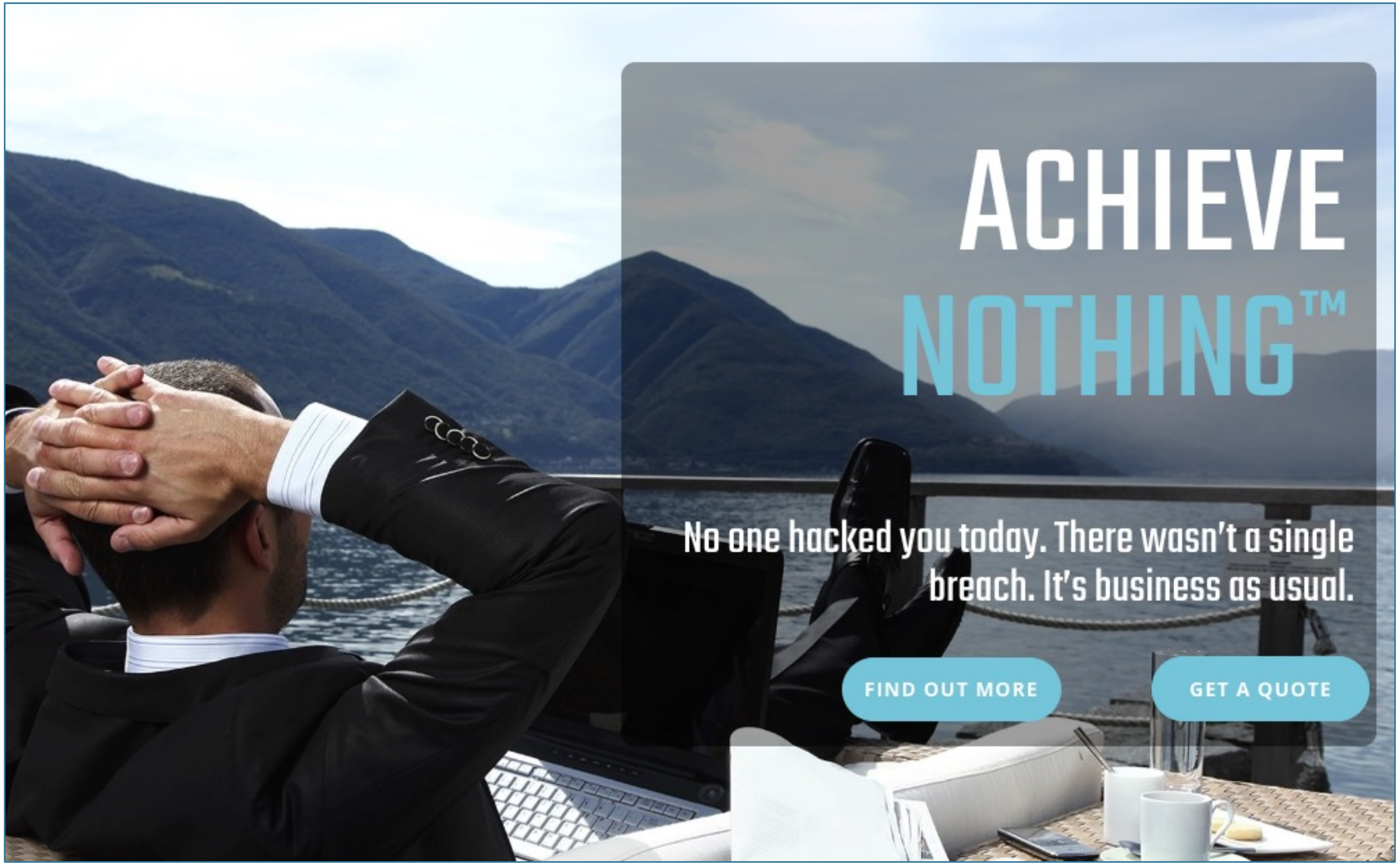
©LMG Security 2021. All rights reserved.

Worldwide Spending on Security & Risk Management Forecast to Grow 11.3% in 2023

Gartner®



The Ultimate Goal of Cybersecurity Spending



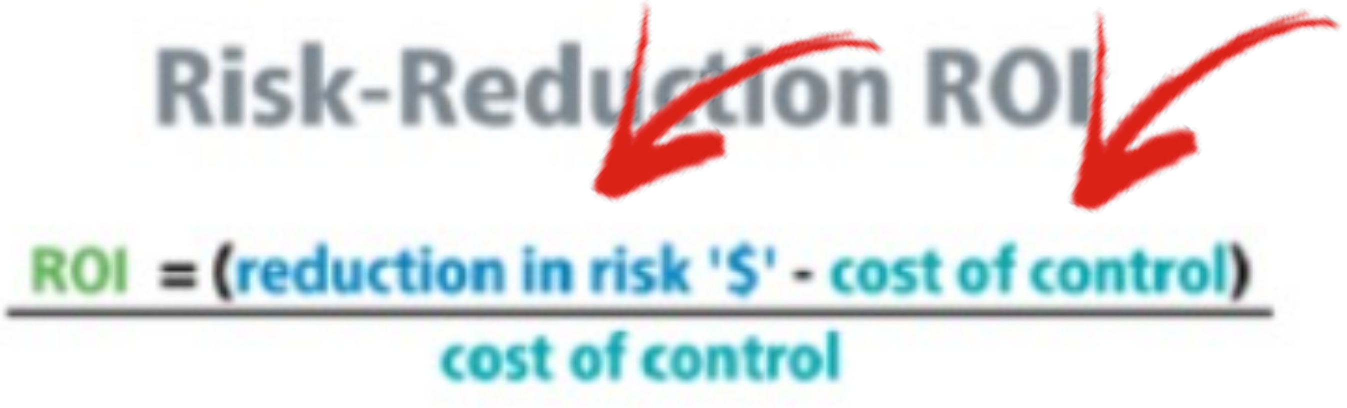
ACHIEVE NOTHING™

No one hacked you today. There wasn't a single breach. It's business as usual.

Getting Return on Investment

Effectively reduce risk!

1. Decrease **likelihood** of a negative event
2. Decrease **impact** of a negative event
3. Spend **efficiently**



Risk-Reduction ROI

$$\text{ROI} = \frac{(\text{reduction in risk '\$'} - \text{cost of control})}{\text{cost of control}}$$

(Risk = impact x likelihood)

Image source: https://www.securitymadesimple.org/cybersecurity-blog/how-to-calculate-the-roi-of-cybersecurity

Running an Effective Cybersecurity Program

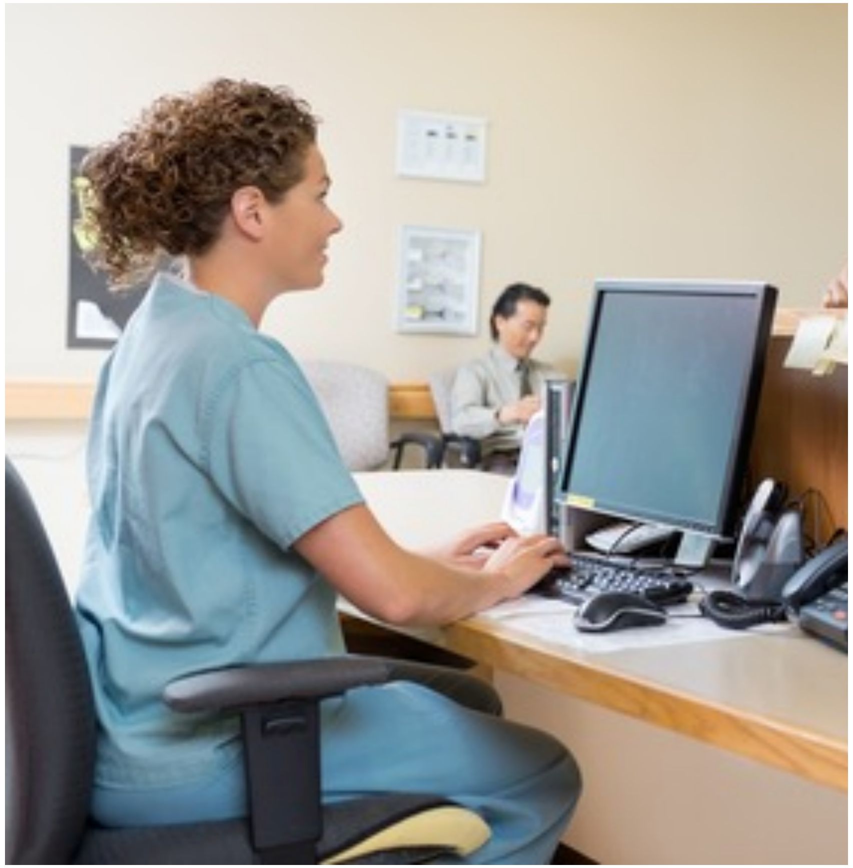
- Know What You’re Trying to Protect
- Understand Your Obligations
- Monitor Your Risk
- Manage Your Risk
  - Top Cybersecurity Controls for 2023

©LMG Security 2021. All rights reserved.

The CIA Triad

- Confidentiality
- Integrity
- Availability

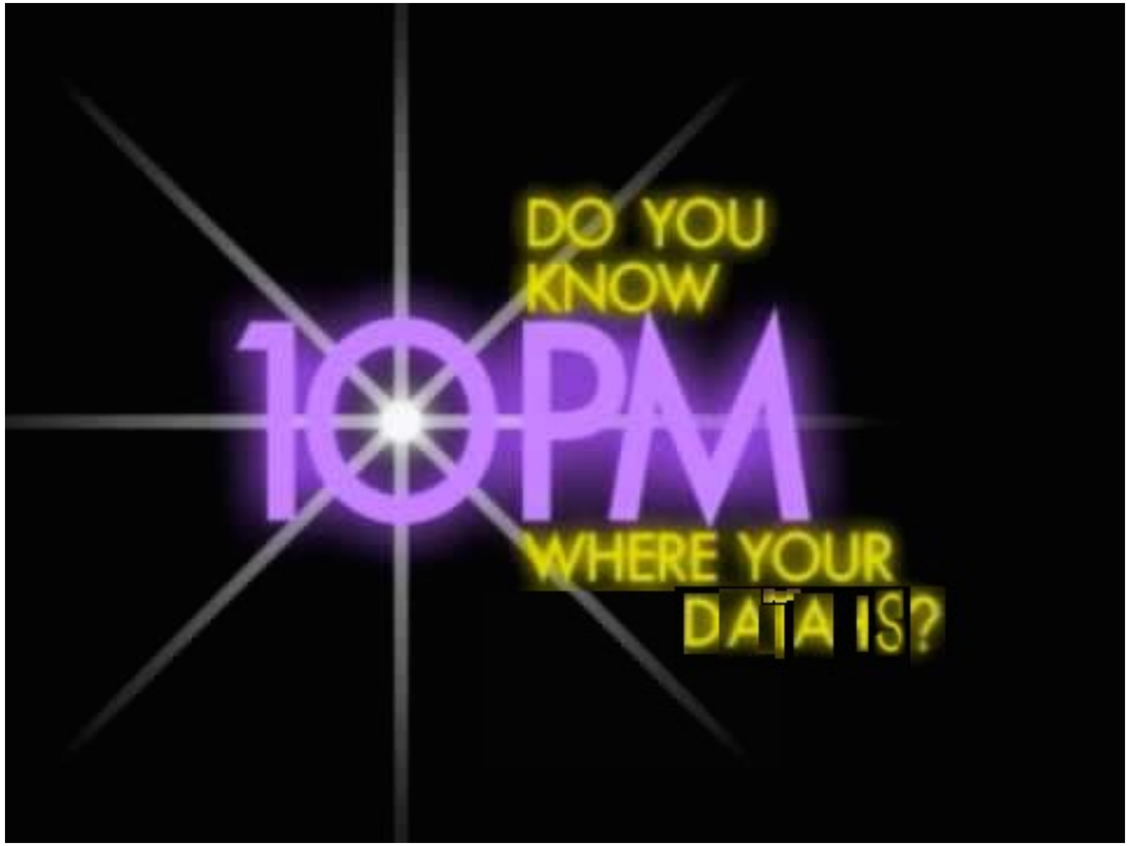
What Systems and Services Do You Need to Protect?



What Data Do You Need to Protect?

- Employee SSNs
- Customer Data
- Tax Returns
- Medical Info
- PII
- Corporate Credit Cards
- Driver’s license scans
- Insurance information

- Intellectual Property
- Confidential Business Information
- Employee and Client Contacts
- IT Asset Inventories
- And more …



Data is Hazardous Material

More Data == More Cost/Risk

Copyright Sherri Davidoff 2018. All rights reserved.

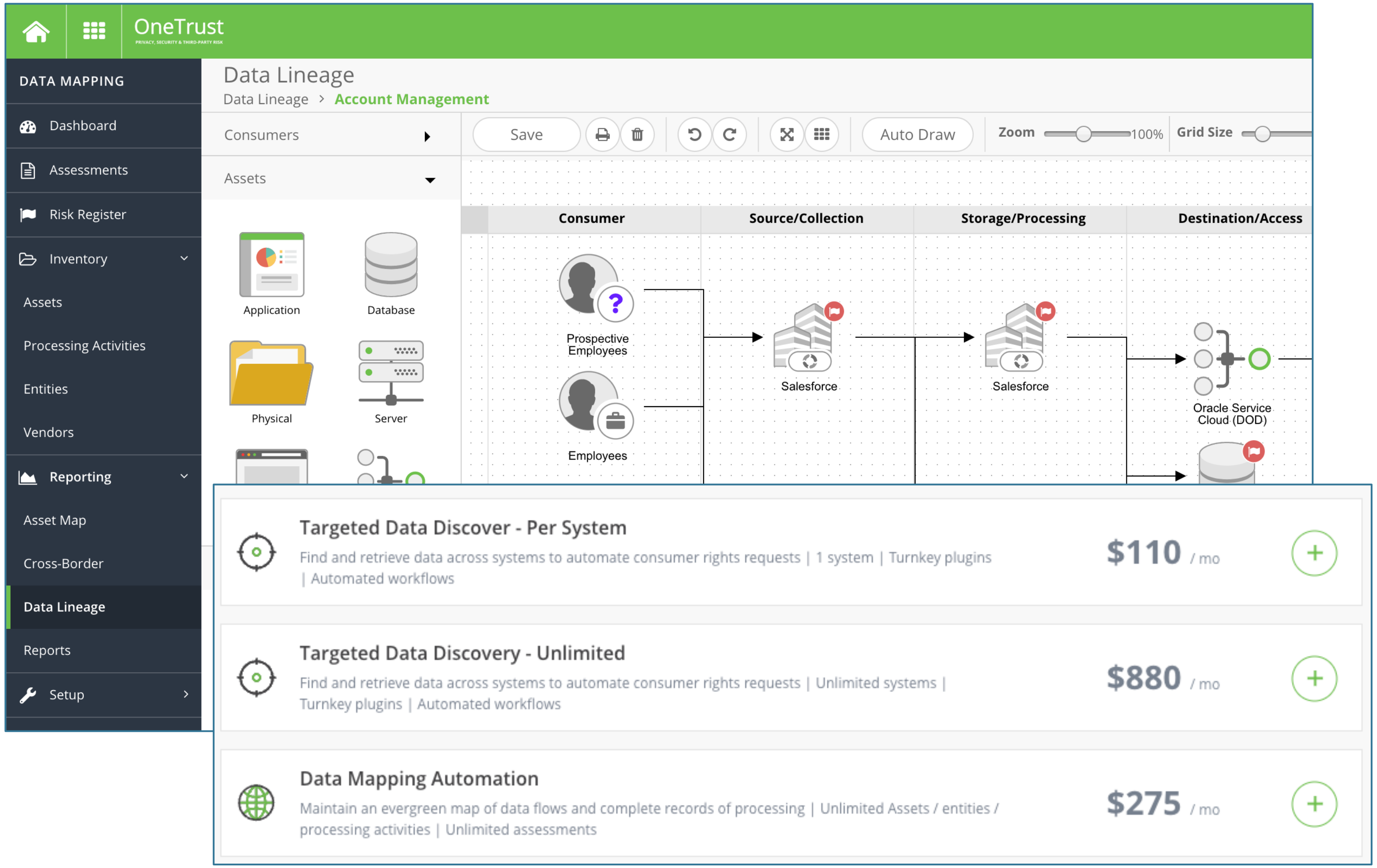
www.LMGsecurity.com

www.LMGsecurity.com

The Cheapest Way to Reduce Your Risk

Routinely Conduct Data Discovery & Mapping

- Identify sensitive data
  - PII
  - Payment card info
  - Passwords
  - & much more
- Local Network & Cloud
  - (Built into some cloud platforms)
- Iterative Process
- Automated Tools



Targeted Data Discover - Per System

Find and retrieve data across systems to automate consumer rights requests | 1 system | Turnkey plugins | Automated workflows

$110 / mo

Targeted Data Discovery - Unlimited

Find and retrieve data across systems to automate consumer rights requests | Unlimited systems | Turnkey plugins | Automated workflows

$880 / mo

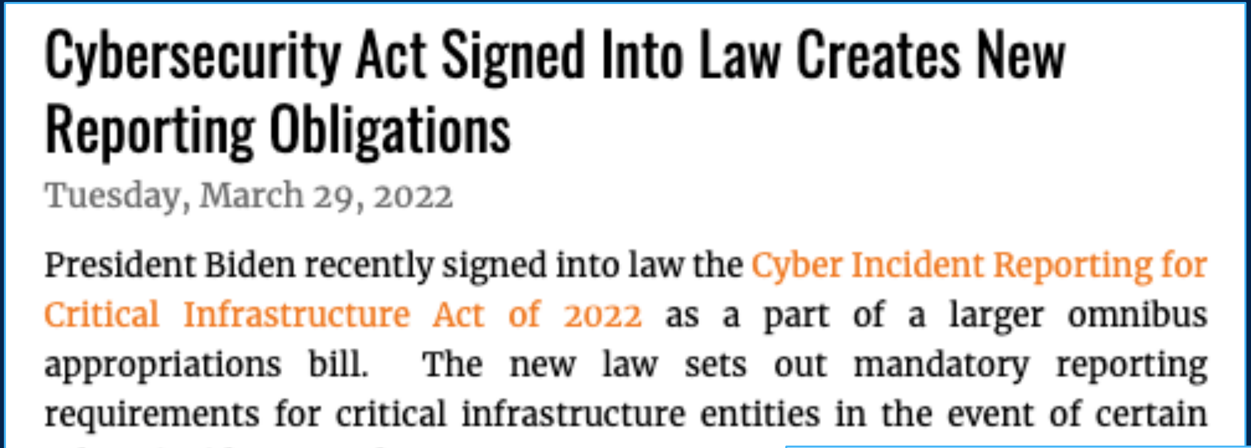
Data Mapping Automation

Maintain an evergreen map of data flows and complete records of processing | Unlimited Assets / entities / processing activities | Unlimited assessments

$275 / mo

Running an Effective Cybersecurity Program

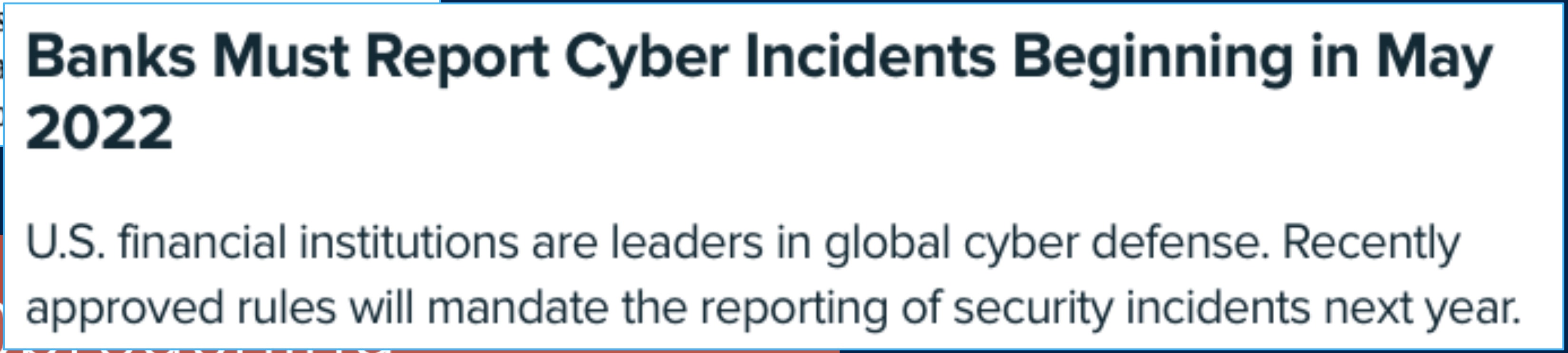
- Know What You're Trying to Protect
- Understand Your Obligations
- Monitor Your Risk
- Manage Your Risk
  - Top Cybersecurity Controls for 2023



Cybersecurity Act Signed Into Law Creates New Reporting Obligations

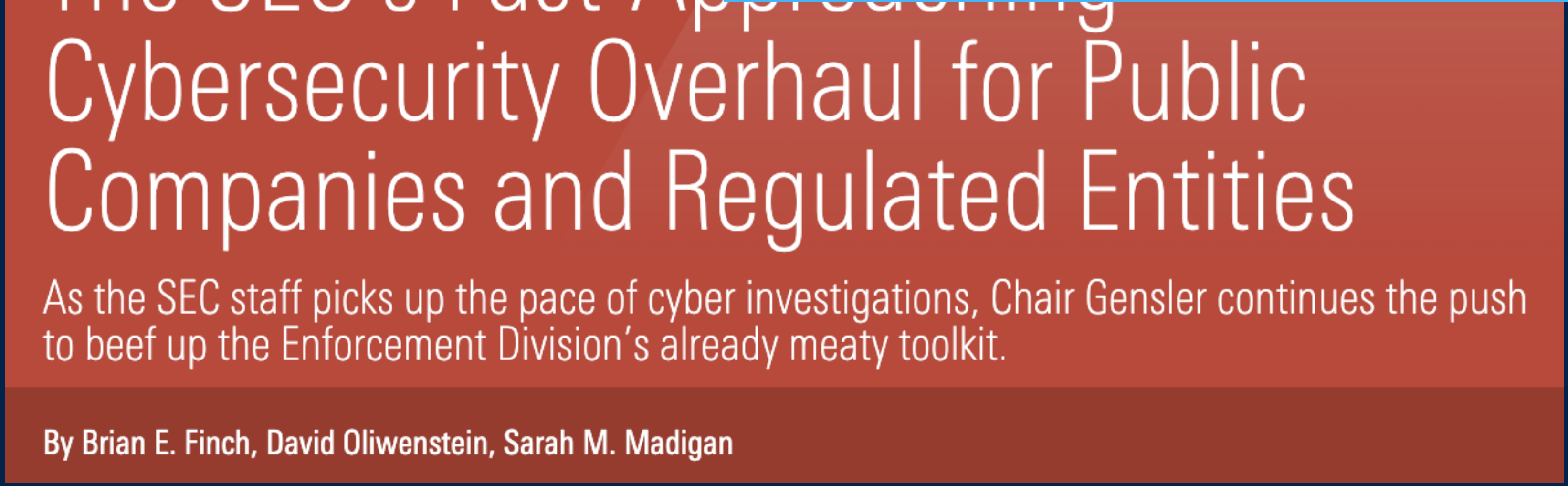
Tuesday, March 29, 2022

President Biden recently signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 as a part of a larger omnibus appropriations bill. The new law sets out mandatory reporting requirements for critical infrastructure entities in the event of certain cyber incidents and ransomware payments
implementing regulations are issued (which a
covered entities will be subject to two new repo



Banks Must Report Cyber Incidents Beginning in May 2022

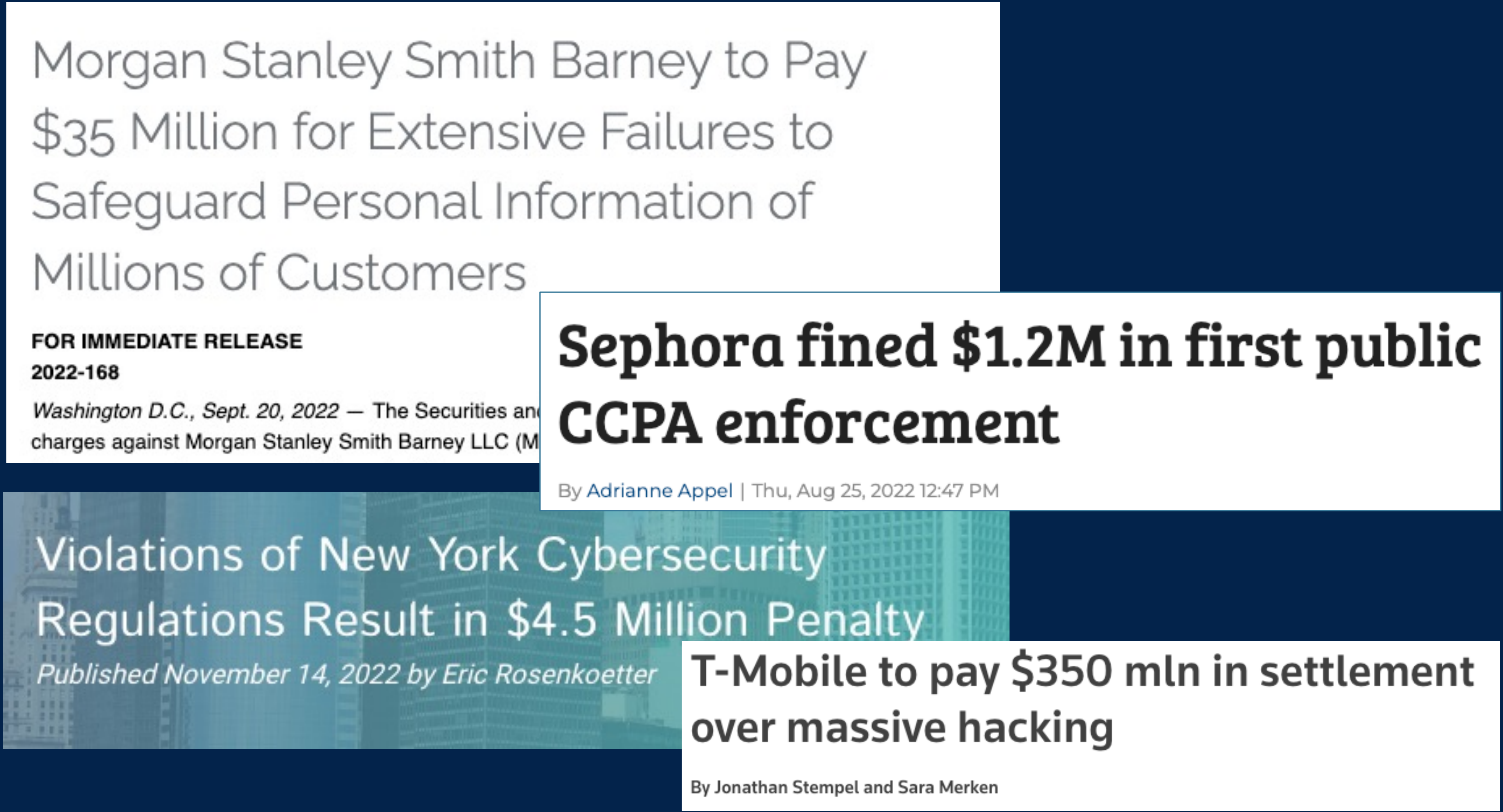
U.S. financial institutions are leaders in global cyber defense. Recently approved rules will mandate the reporting of security incidents next year.



The SEC's Fast-Ap Cybersecurity Overhaul for Public Companies and Regulated Entities

As the SEC staff picks up the pace of cyber investigations, Chair Gensler continues the push to beef up the Enforcement Division's already meaty toolkit.

By Brian E. Finch, David Oliwenstein, Sarah M. Madigan



Morgan Stanley Smith Barney to Pay $35 Million for Extensive Failures to Safeguard Personal Information of Millions of Customers

FOR IMMEDIATE RELEASE
2022-168

Washington D.C., Sept. 20, 2022 — The Securities an
charges against Morgan Stanley Smith Barney LLC (M

Sephora fined $1.2M in first public CCPA enforcement

By Adrianne Appel | Thu, Aug 25, 2022 12:47 PM

Violations of New York Cybersecurity Regulations Result in $4.5 Million Penalty

Published November 14, 2022 by Eric Rosenkoetter

T-Mobile to pay $350 mln in settlement over massive hacking

By Jonathan Stempel and Sara Merken

Consult a Qualified Data Privacy Lawyer

- Statement of Application Laws, Regulations and Obligations
- Oversight Responsibilities
- Outsource these decisions
  - (Lowers your risk)
- Laws evolve rapidly
- Highly specialized industry
- Annual review

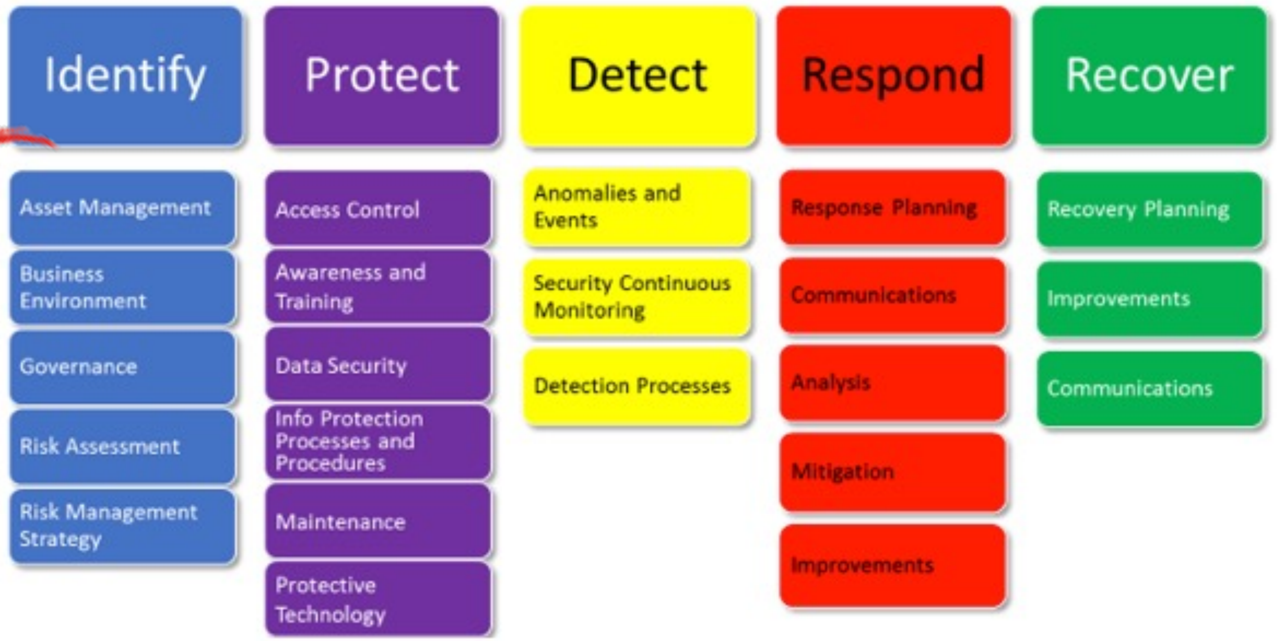
©LMG Security 2021. All rights reserved.

Running an Effective Cybersecurity Program

- Know What You’re Trying to Protect
- Understand Your Obligations
- Monitor Your Risk
- Manage Your Risk
  - Top Cybersecurity Controls for 2023

Monitoring Risk

1. Cybersecurity controls assessment
2. Technical testing
3. Risk assessment
4. Incident review



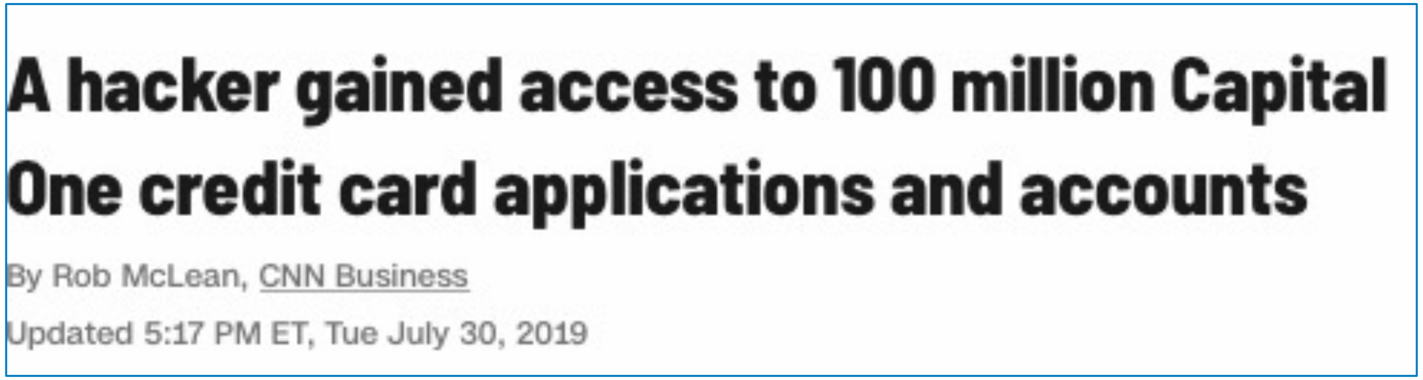
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications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

NIST Cybersecurity Framework

Conduct Technical Testing

- Penetration Testing
- Vulnerability Scans
- Phishing Tests
- Threat Hunting
- Cloud Config Reviews

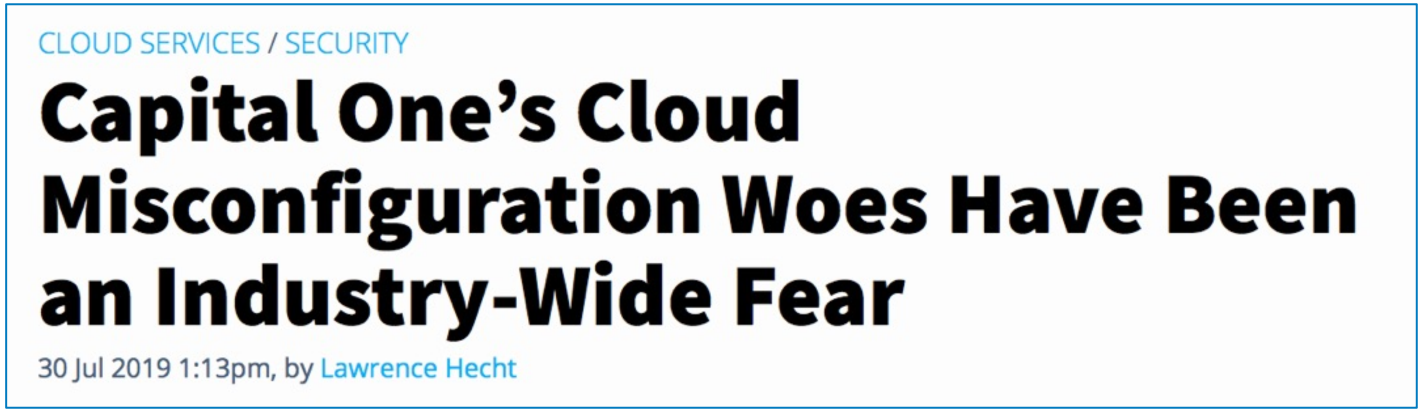
Align with Your Current Environment & Current Threats



A hacker gained access to 100 million Capital One credit card applications and accounts

By Rob McLean, CNN Business

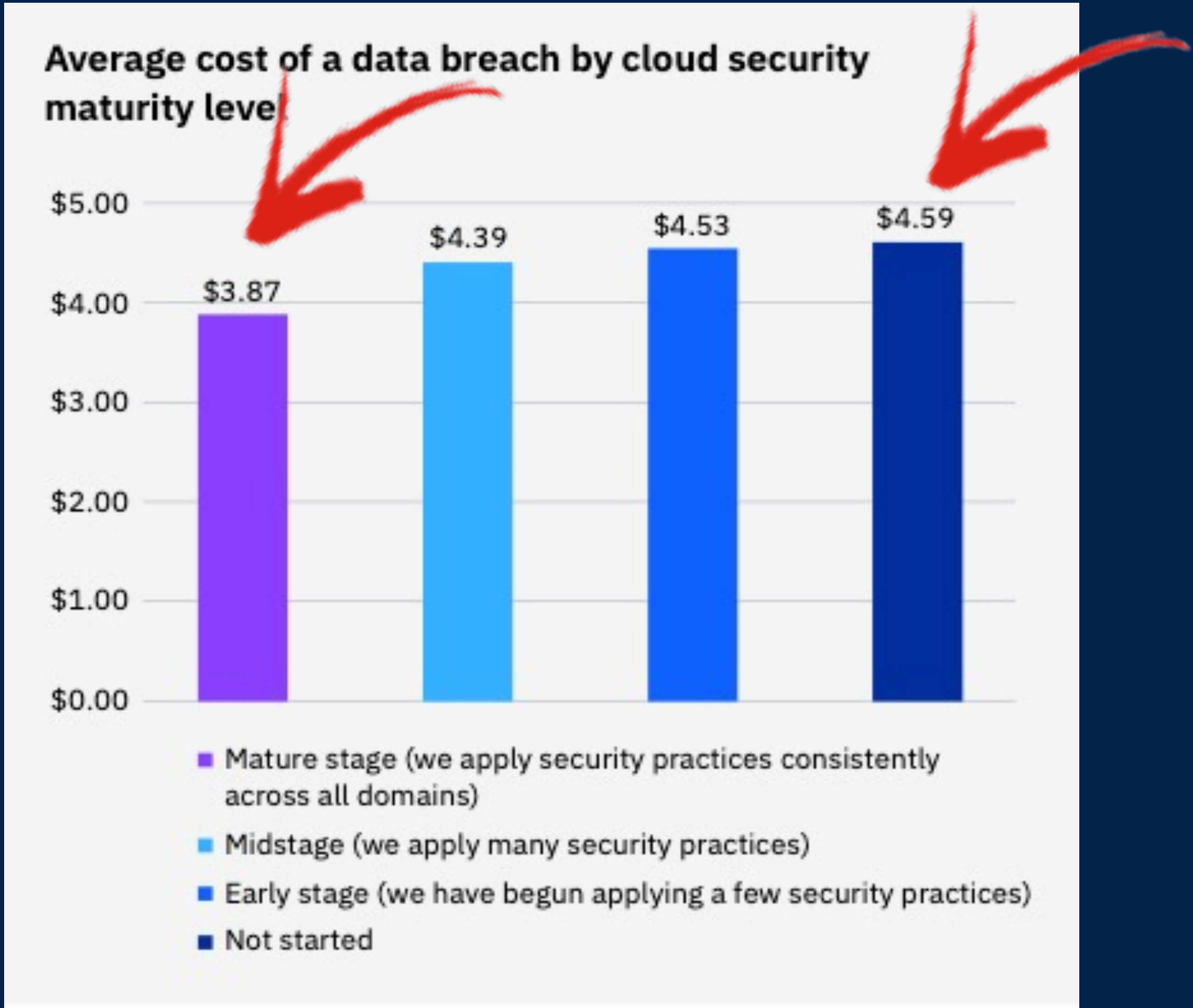
Updated 5:17 PM ET, Tue July 30, 2019



CLOUD SERVICES / SECURITY

Capital One's Cloud Misconfiguration Woes Have Been an Industry-Wide Fear

30 Jul 2019 1:13pm, by Lawrence Hecht



Average cost of a data breach by cloud security maturity level

igure 44: Measured in USD millions

45%

of the breaches were cloud-based.

IBM

☑ Conduct Cloud Configuration Reviews

- ✓Inventory your cloud apps & data
- ✓Prioritize based on criticality & data sensitivity
  - ie M365, Sharepoint, GCP
- ✓Conduct routine config reviews
  - Prevent BEC attacks, data breaches
- ✓Integrate with security products
- ✓Monitor alerts & notifications

Manage Your Risk

- Know What You’re Trying to Protect
- Understand Your Obligations
- Monitor Your Risk
- Manage Your Risk
  - Top Cybersecurity Controls for 2023

3 Factors to Consider When Budgeting

A. **What is your risk?**
   - Consider emerging threats
   - Compliance / contractual requirements

B. **What is your organization's risk <u>appetite</u>?**

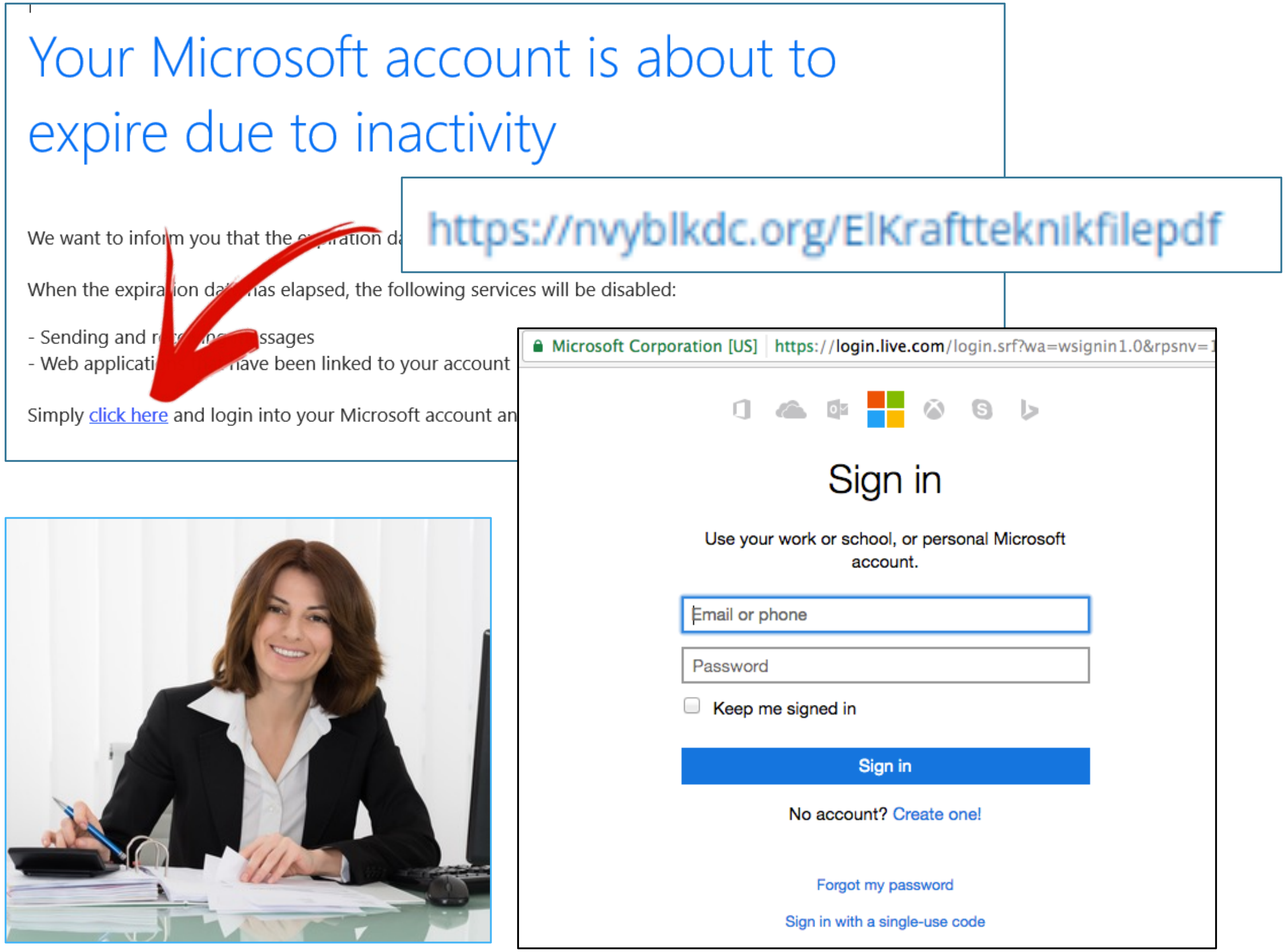
C. **How much do you need to spend to get risk to a level where your organization is comfortable?**

Case Study: Missed Payment

- Manufacturing Company
- Received notification that a payment to their insurance had not been received
- Bookkeeper sent the payment two weeks prior ($160K)
- Payment was never received

What Happened?

- New Bookkeeper
  - Only on staff for about 90 days
- Received a phishing email
- Entered credentials on a lookalike Microsoft O365 login page
- Adversary from Estonia accessed the account and redirected payment
- **Money is gone!**



Your Microsoft account is about to expire due to inactivity

We want to inform you that the expiration d

When the expiration date has elapsed, the following services will be disabled:

- Sending and receiving messages
- Web applications that have been linked to your account

Simply click here and login into your Microsoft account an

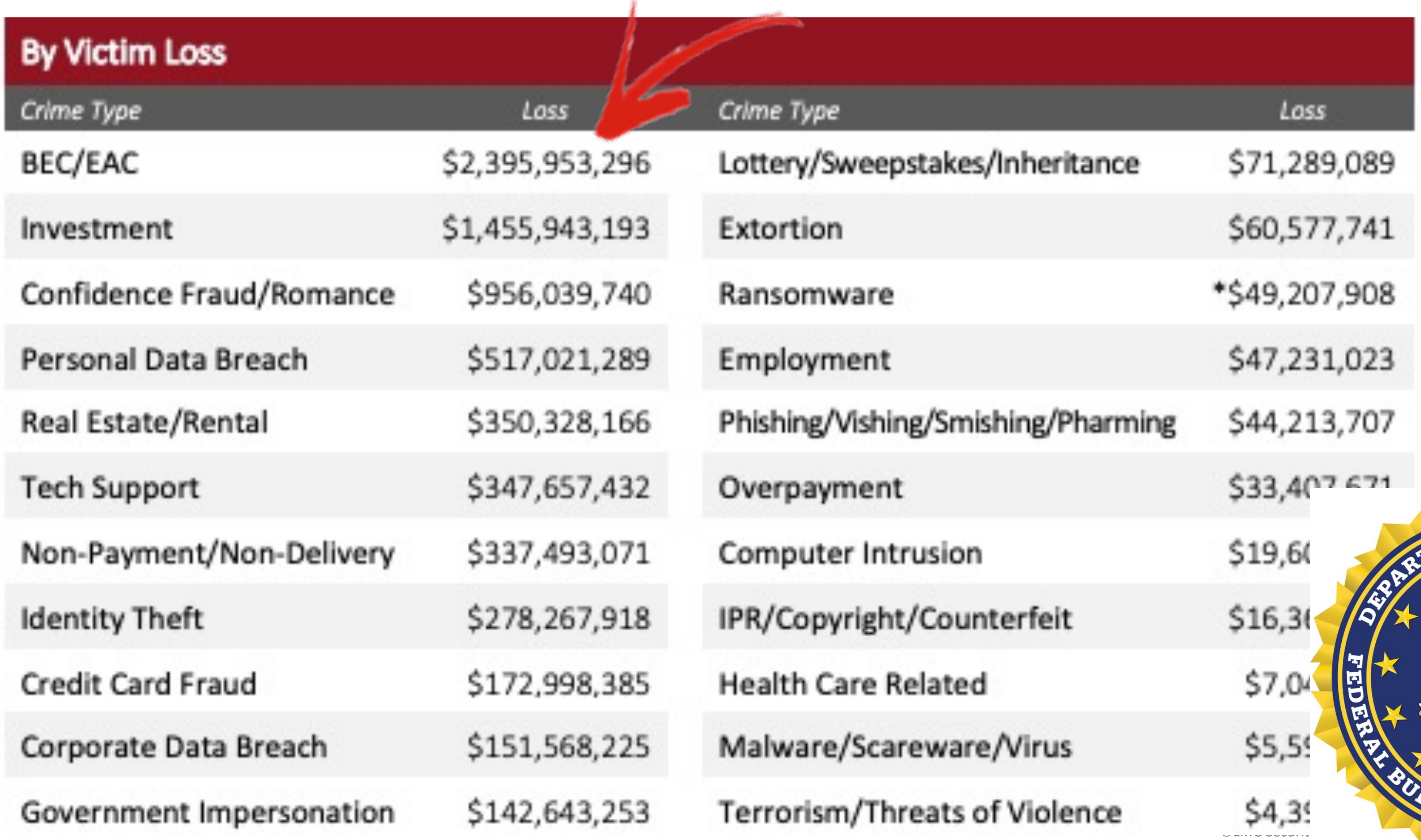
https://nvyblkdc.org/ElKraftteknikfilepdf

Microsoft Corporation [US] | https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=1

Sign in

Use your work or school, or personal Microsoft account.

Business Email Compromise is the #1 Crime By $$

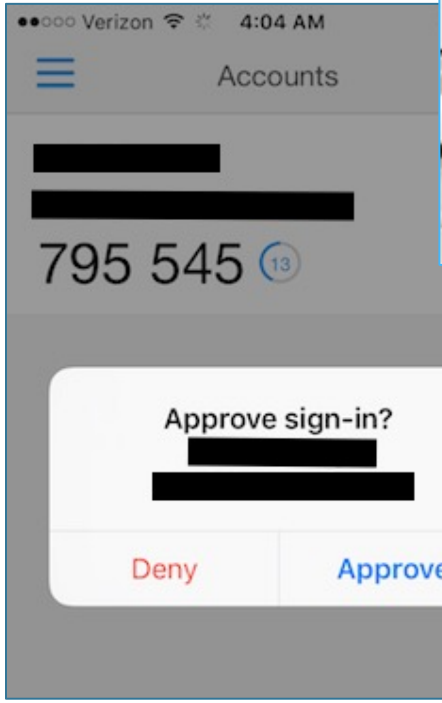


By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/Romance	$956,039,740	Ransomware	*$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$44,213,707
Tech Support	$347,657,432	Overpayment	$33,407,671
Non-Payment/Non-Delivery	$337,493,071	Computer Intrusion	$19,60
Identity Theft	$278,267,918	IPR/Copyright/Counterfeit	$16,36
Credit Card Fraud	$172,998,385	Health Care Related	$7,04
Corporate Data Breach	$151,568,225	Malware/Scareware/Virus	$5,59
Government Impersonation	$142,643,253	Terrorism/Threats of Violence	$4,39

Use Multifactor Authentication

- Authenticate = verify identity
  - Something you know (Type 1)
  - Something you have (Type 2)
  - Something you are (Type 3)
- Multifactor = more than one



●●○○○ Verizon 4:04 AM

Accounts

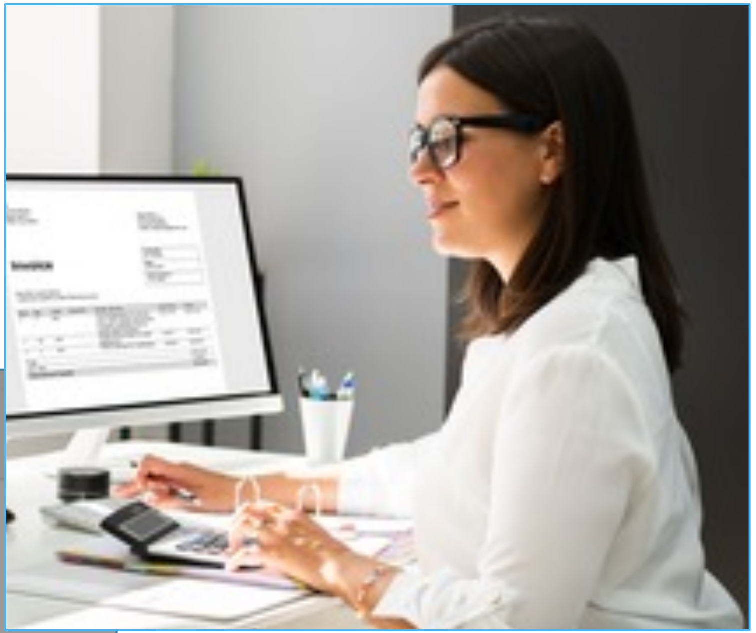
[redacted]

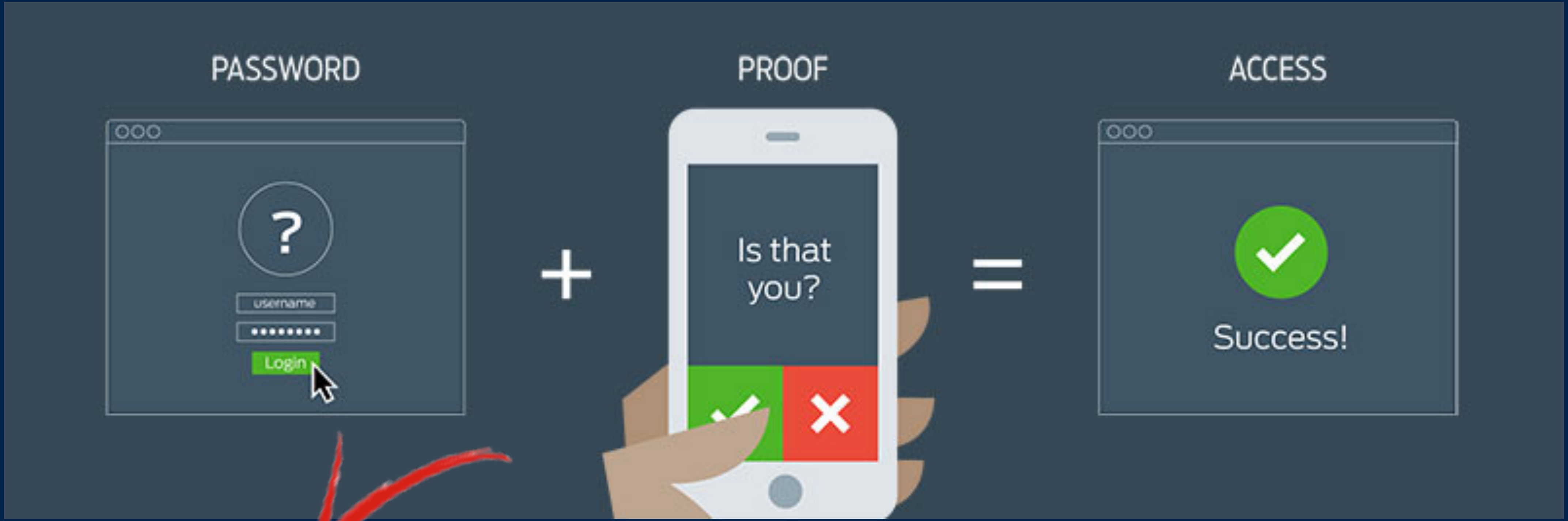
795 545 13

Approve sign-in?

[redacted]

Deny Approve

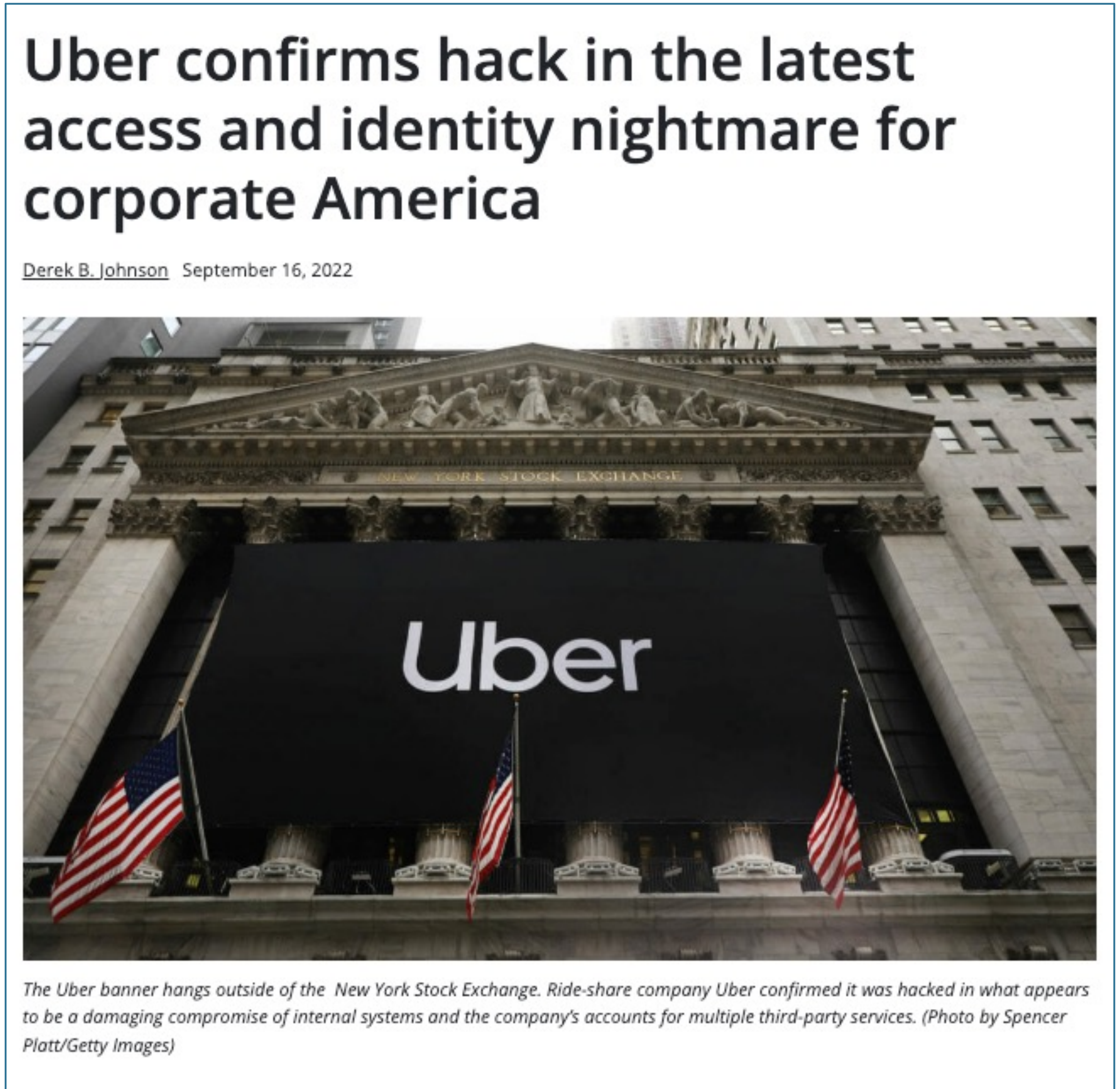




Duo MFA	Duo Access	Duo Beyond
$3 / User / Month	$6 / User / Month	$9 / User / Month

Case Study: The Uber Hack

- Hacker broke into Uber’s corporate IT environment
- Gained full access to key servers and cloud platforms
- Posted screenshots & told media
- Hacker claims to be an 18-year-old
- Currently Uber says the “production” systems and sensitive user info is not affected
  - (Investigation is ongoing)



Uber confirms hack in the latest access and identity nightmare for corporate America

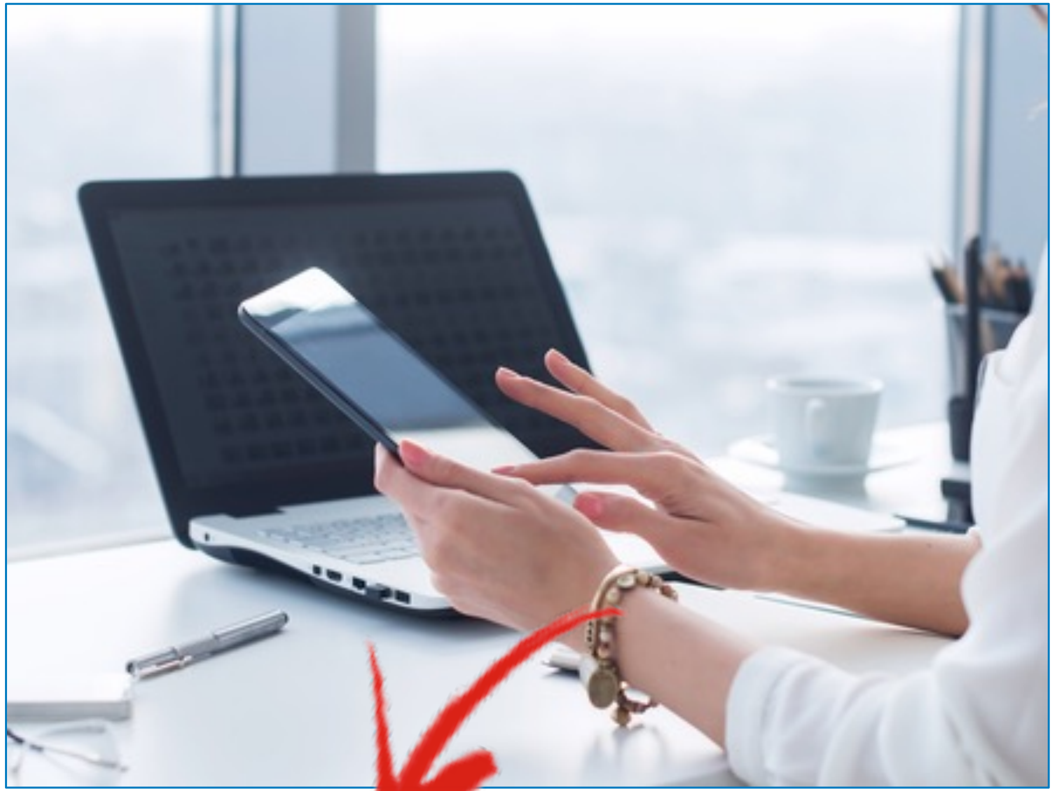
Derek B. Johnson September 16, 2022

The Uber banner hangs outside of the New York Stock Exchange. Ride-share company Uber confirmed it was hacked in what appears to be a damaging compromise of internal systems and the company’s accounts for multiple third-party services. (Photo by Spencer Platt/Getty Images)

How They Got Hacked

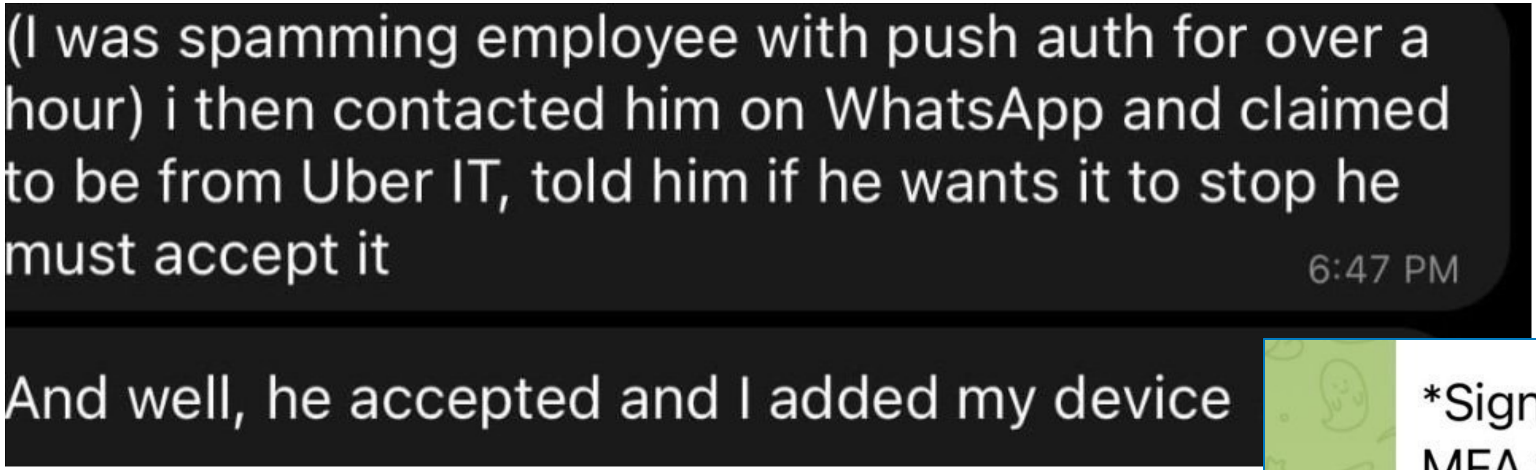
- Likely started with a contractor’s **<u>hacked personal device</u>**
  - “infected with malware” (Uber 9/16/22)
- Corporate password sold on dark web
- Purchased & attackers tried to log in repeatedly
  - MFA blocked access
  - **THWARTED!**

(But wait, there’s more…)



There are 24.6 billion pairs of credentials for sale on dark web

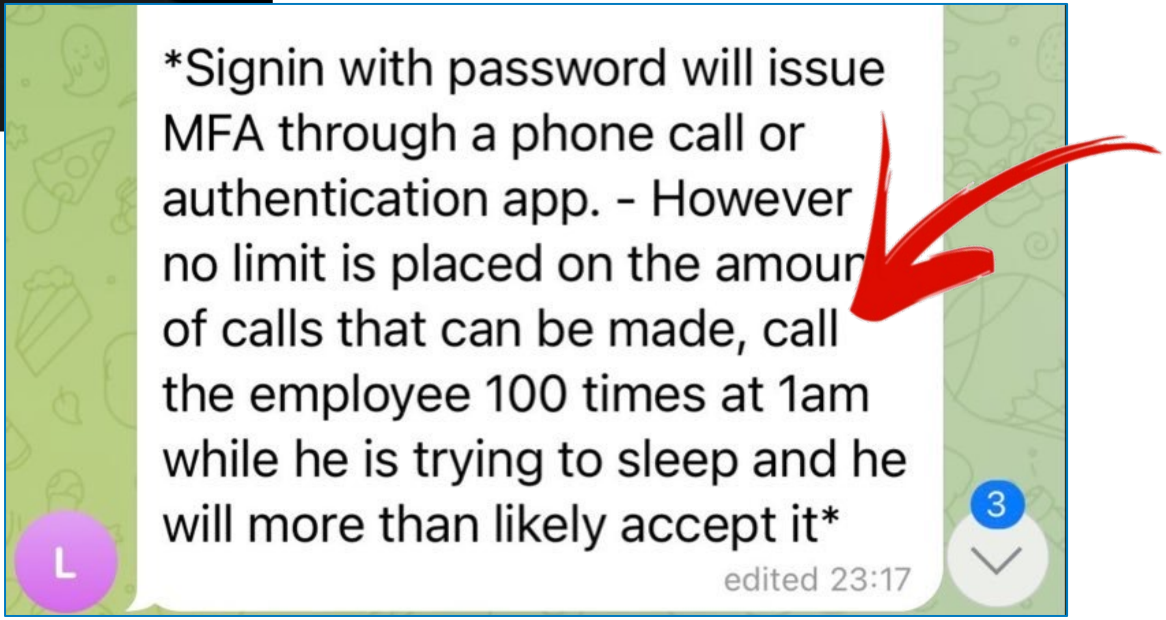
Hacker Bombarded the User's Phone



(I was spamming employee with push auth for over a hour) i then contacted him on WhatsApp and claimed to be from Uber IT, told him if he wants it to stop he must accept it 6:47 PM

And well, he accepted and I added my device

“MFA fatigue” is real!



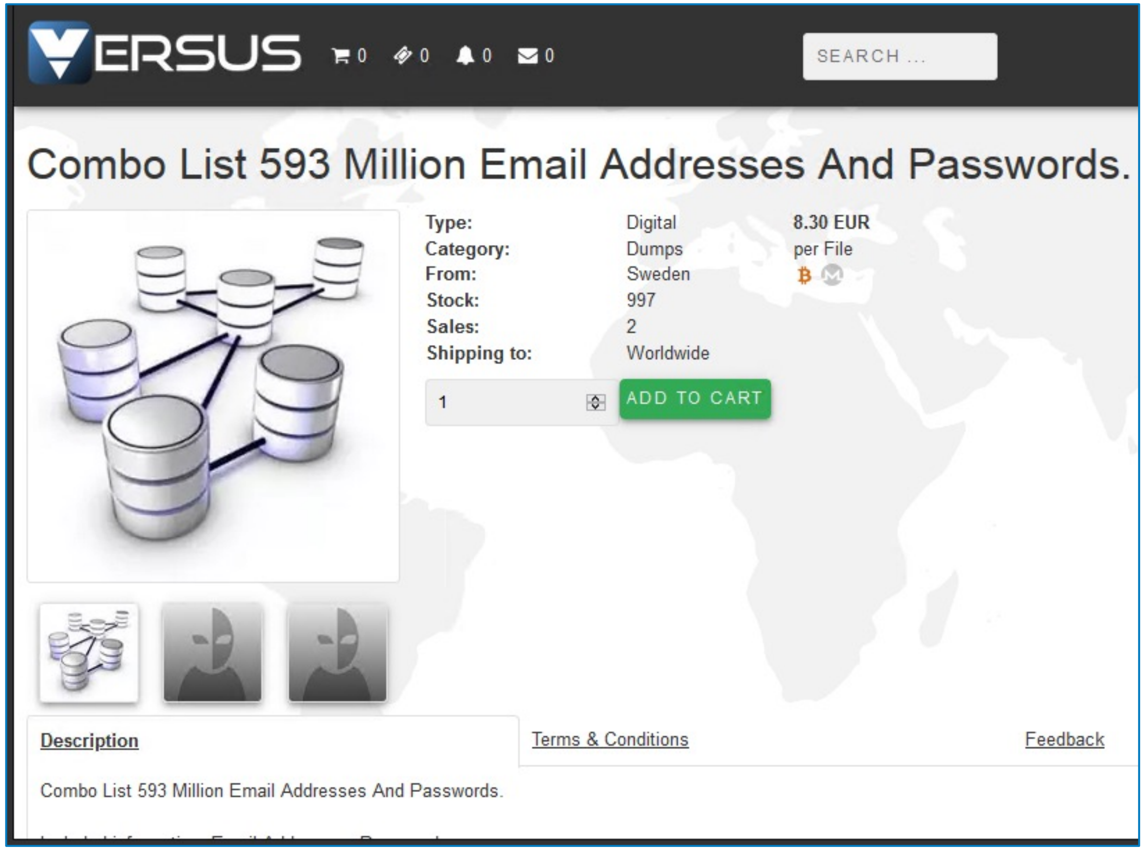
Signin with password will issue MFA through a phone call or authentication app. - However no limit is placed on the amount of calls that can be made, call the employee 100 times at 1am while he is trying to sleep and he will more than likely accept it

edited 23:17

https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/

Hackers Can Get Your Cell Phone

- Two researchers presented at Black Hat USA (Aug 2022)
- Searched the dark web for stolen passwords
- Found databases of cell phone numbers
- Linked together to get a data base with over 1 BILLION stolen passwords + phone #s



Combo List 593 Million Email Addresses And Passwords.

Type:	Digital	8.30 EUR
Category:	Dumps	per File
From:	Sweden	
Stock:	997	
Sales:	2	
Shipping to:	Worldwide	

Description | Terms & Conditions | Feedback

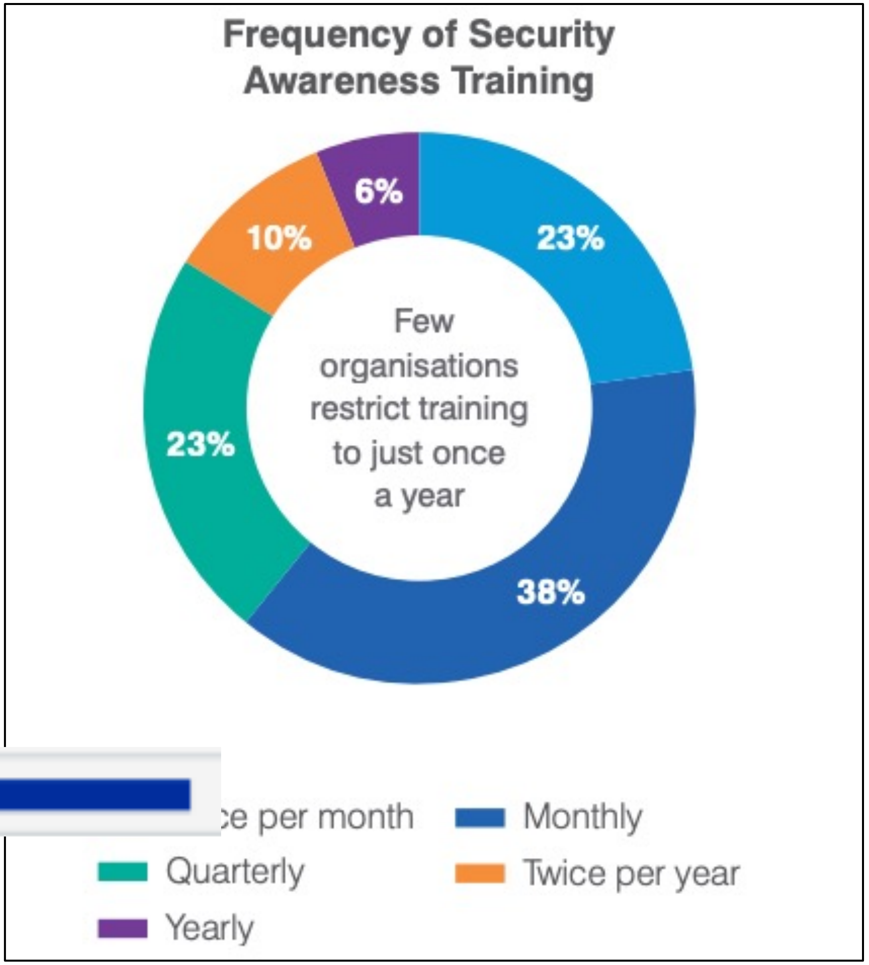
Combo List 593 Million Email Addresses And Passwords.

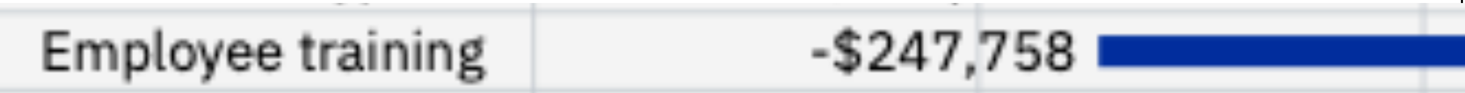
https://www.darkreading.com/cloud/stolen-data-attackers-advantage-text-based-2fa

©LMG Security 2021. All rights reserved.

Conduct Cybersecurity Awareness Training

- On-Demand Awareness Videos
- Email Reminders
- Phishing Exercises
- <u>Include MFA social engineering attacks</u>
  - Texts & phone calls



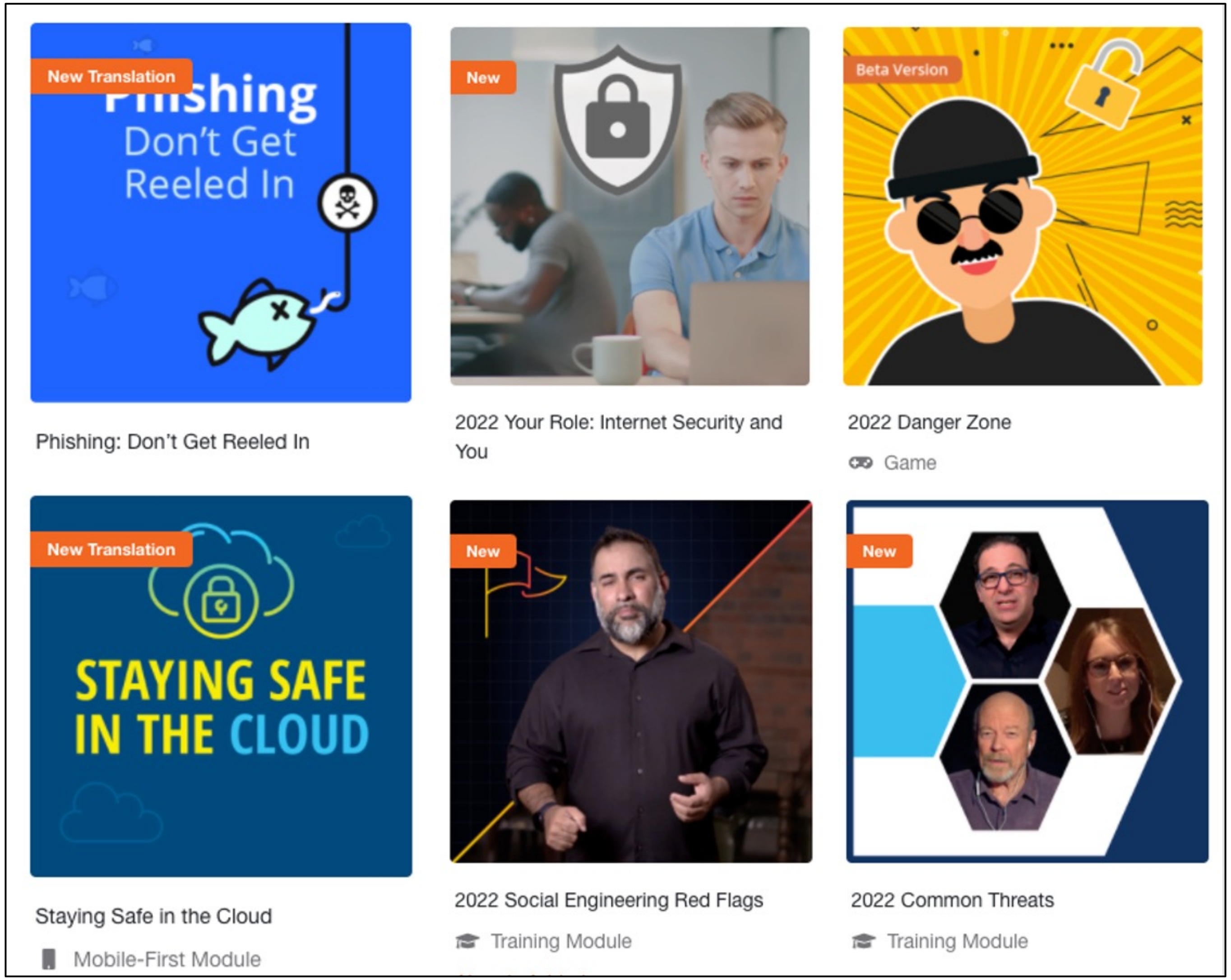


Employee training	-$247,758

On-Demand Training Portal

- Strengthen your human firewall
- Keep cyber top of mind
- Example: KnowBe4 Platform
- Over 1,350 Training Modules
- Includes phishing tests
- Highly effective!

PCBS Community Discount on KnowBe4 Training Platform through March 30!
Email info@LMGsecurity.com



Phishing: Don't Get Reeled In

2022 Your Role: Internet Security and You

2022 Danger Zone
Game

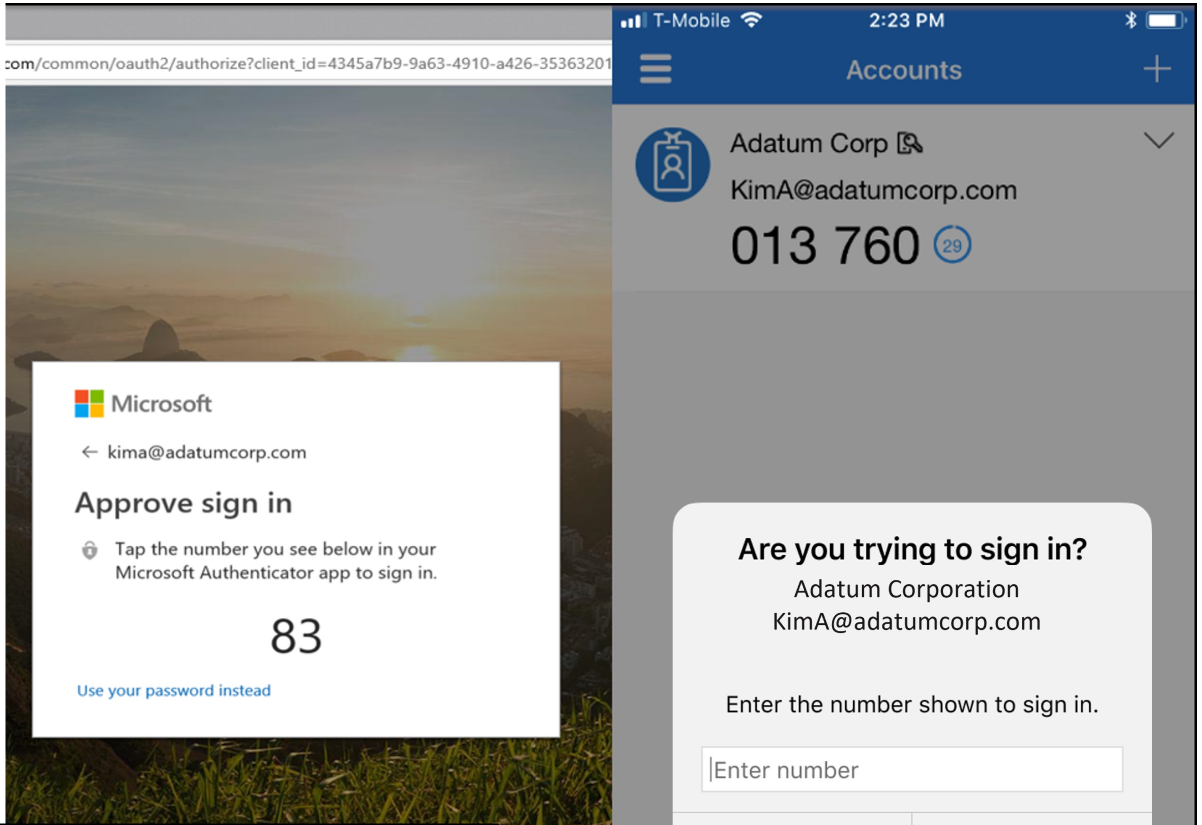
Staying Safe in the Cloud
Mobile-First Module

2022 Social Engineering Red Flags
Training Module

2022 Common Threats
Training Module

Use Strong MFA

- Choose a strong method
  - ie Hardware token or App
  - NOT SMS/email/phone
- Configure carefully!



com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201

Microsoft

← kima@adatumcorp.com

Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

83

Use your password instead

T-Mobile 2:23 PM

Accounts

Adatum Corp

KimA@adatumcorp.com

013 760 29

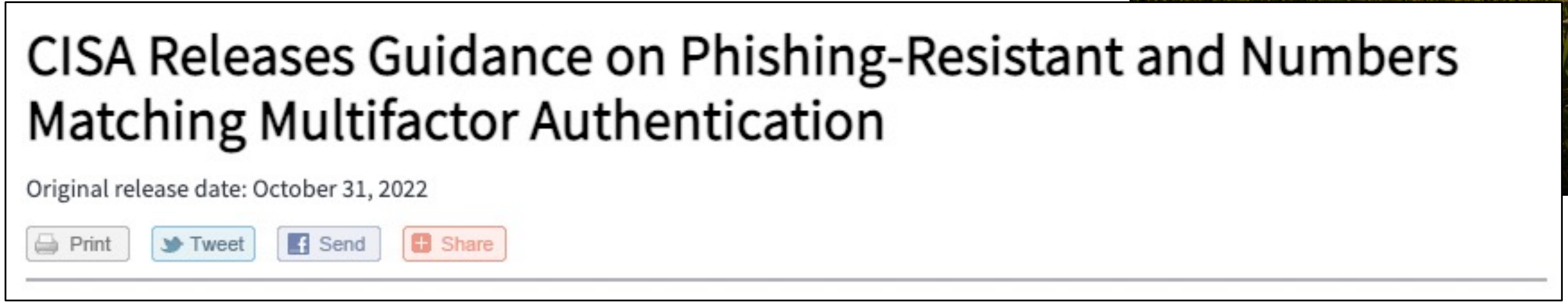
Are you trying to sign in?

Adatum Corporation

KimA@adatumcorp.com

Enter the number shown to sign in.

Enter number

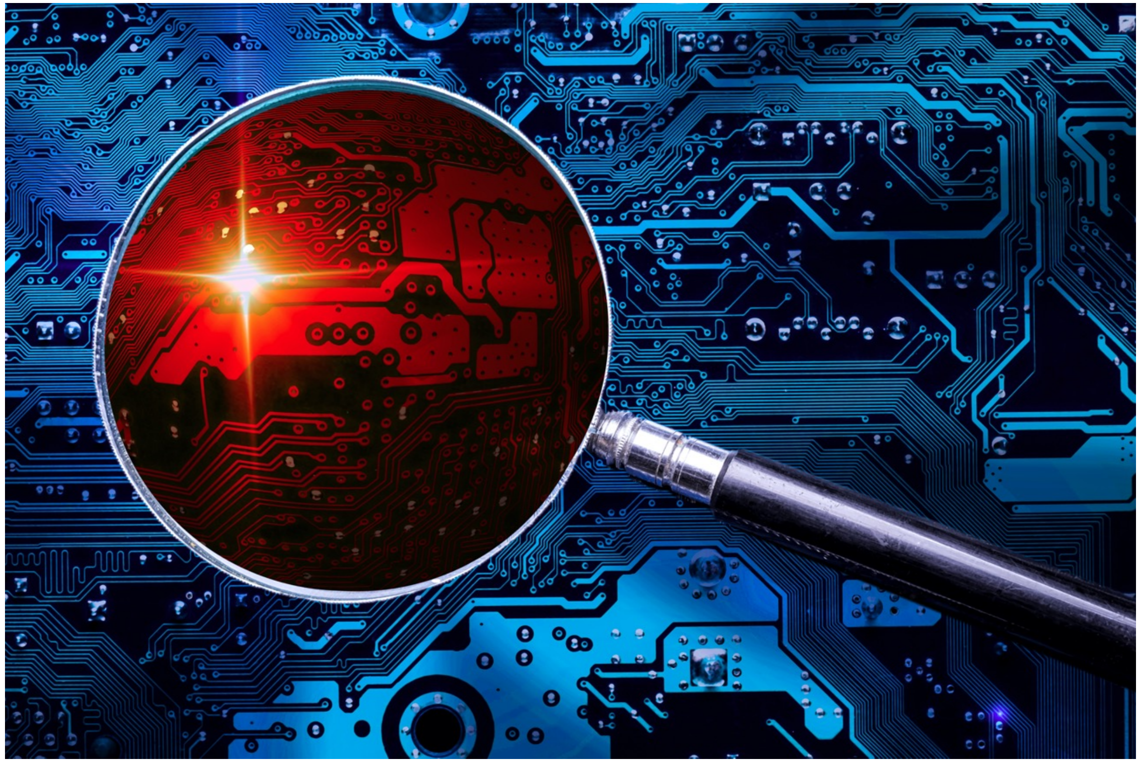


CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication

Original release date: October 31, 2022

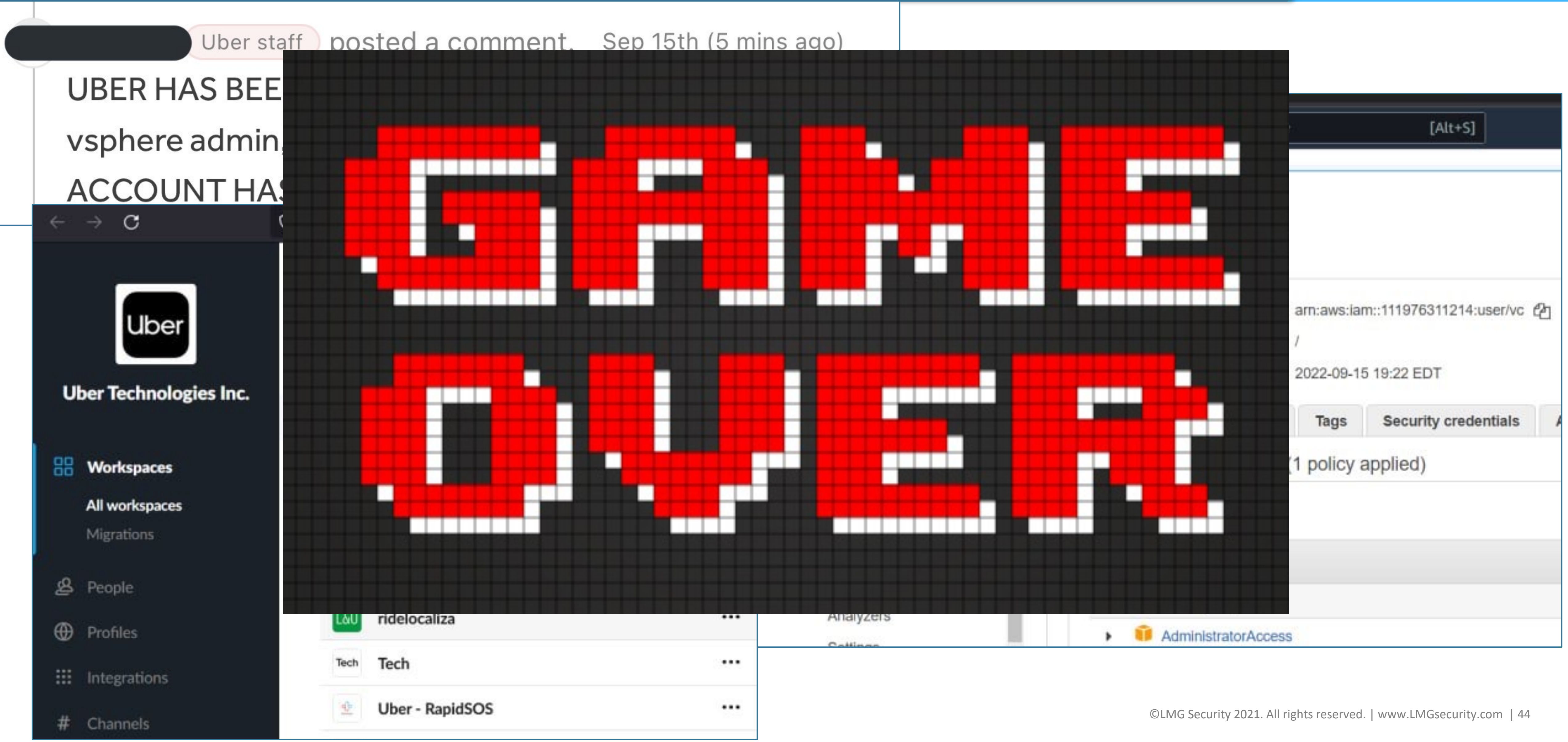
Once The Hackers Were Inside Uber's Network…

- Expanded access to other employee accounts and computers
- Gained access to core servers
- Reconfigured network to "display a graphic image to employees"



https://www.uber.com/newsroom/security-update

The Hackers Quickly Jumped to the Cloud



[redacted] Uber staff posted a comment. Sep 15th (5 mins ago)

UBER HAS BEE

vsphere admin

ACCOUNT HAS

arn:aws:iam::111976311214:user/vc

/

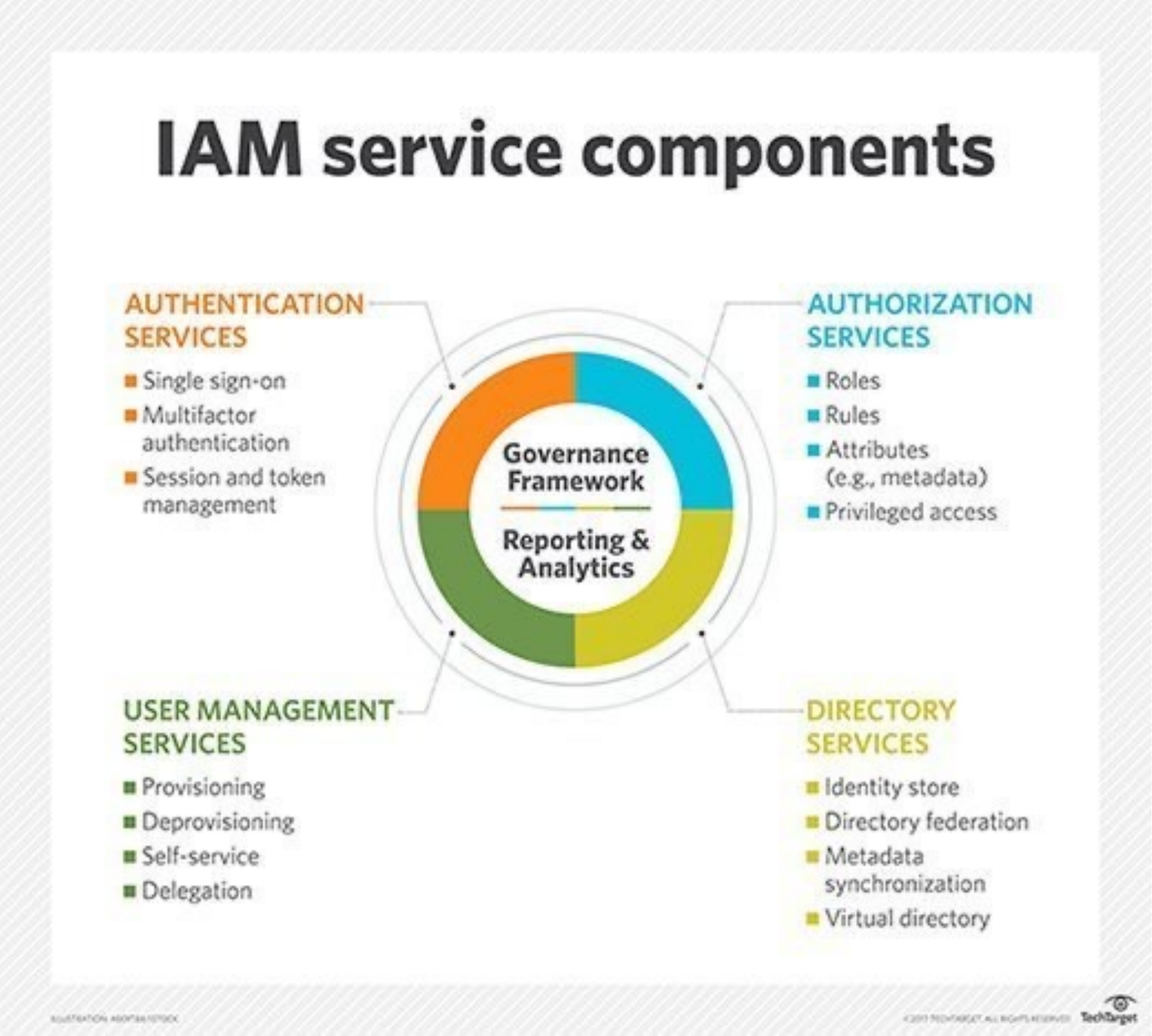
2022-09-15 19:22 EDT

(1 policy applied)

AdministratorAccess

Identity and Access Management

- Restrict access to accounts
- If an account is misused/used inappropriate
- Supports automated response
- Can act as a central identity provider for other services



IAM service components

AUTHENTICATION SERVICES
- Single sign-on
- Multifactor authentication
- Session and token management

AUTHORIZATION SERVICES
- Roles
- Rules
- Attributes (e.g., metadata)
- Privileged access

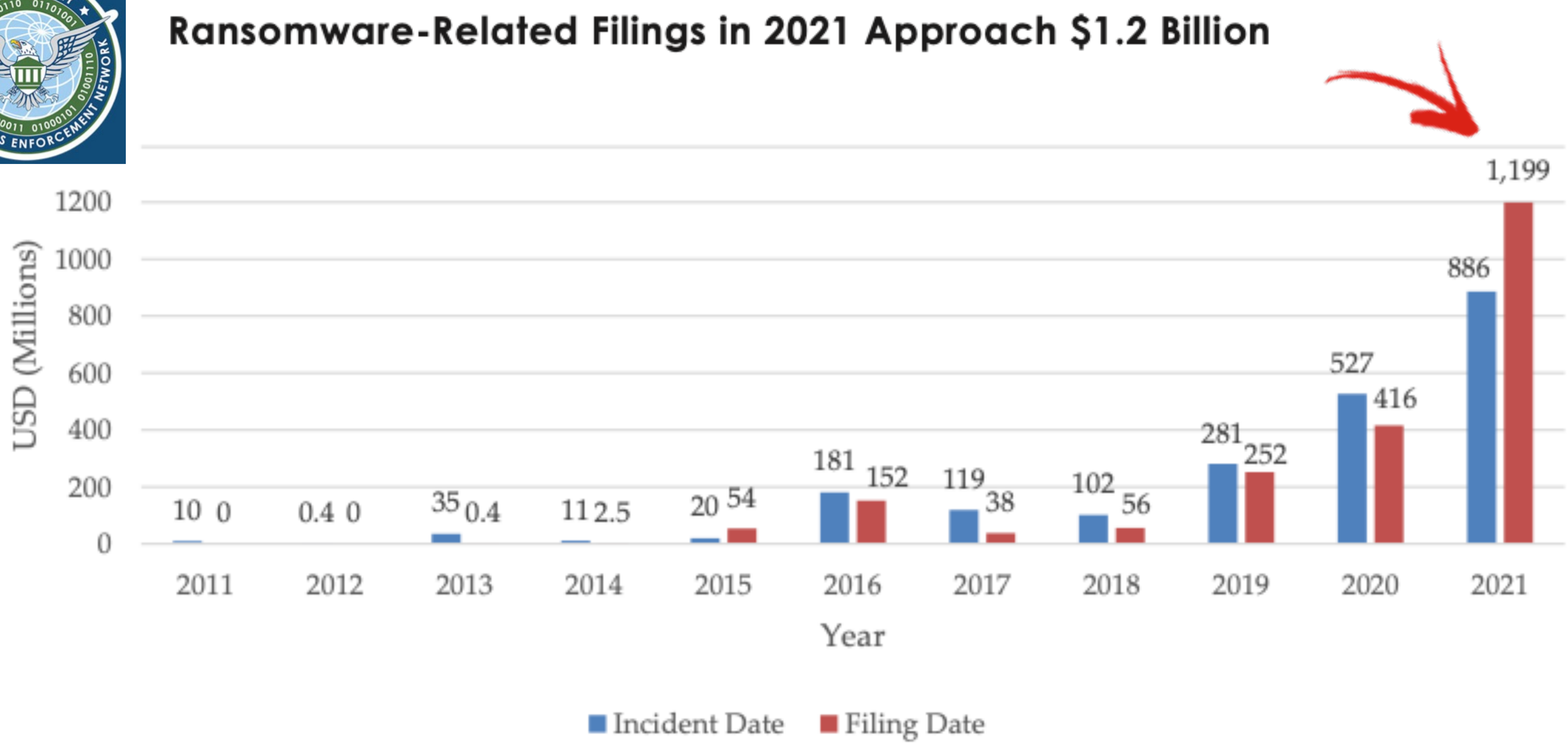
Governance Framework

Reporting & Analytics

USER MANAGEMENT SERVICES
- Provisioning
- Deprovisioning
- Self-service
- Delegation

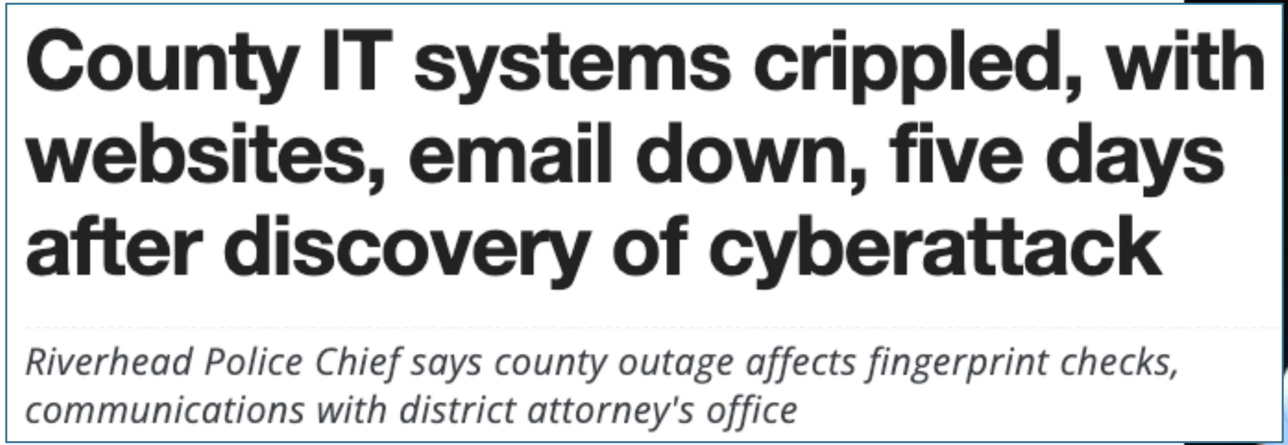
DIRECTORY SERVICES
- Identity store
- Directory federation
- Metadata synchronization
- Virtual directory

Ransomware Remains a Top Threat



Ransomware-Related Filings in 2021 Approach $1.2 Billion

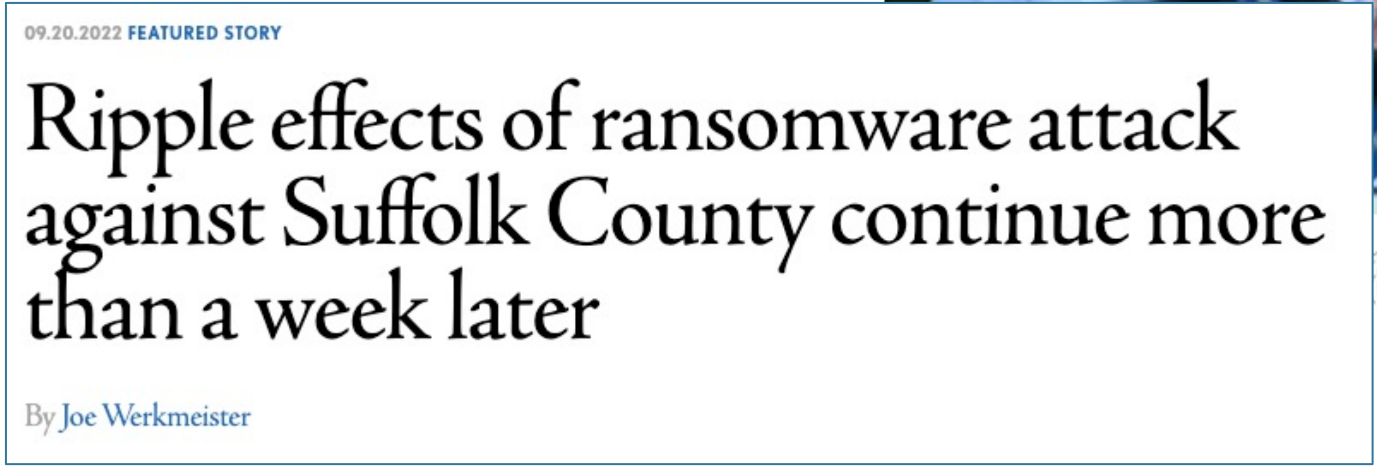
Case Study: BlackCat Attack!



County IT systems crippled, with websites, email down, five days after discovery of cyberattack

Riverhead Police Chief says county outage affects fingerprint checks, communications with district attorney's office

y Harrison discusses the
(Credit: Joe Werkmeister)



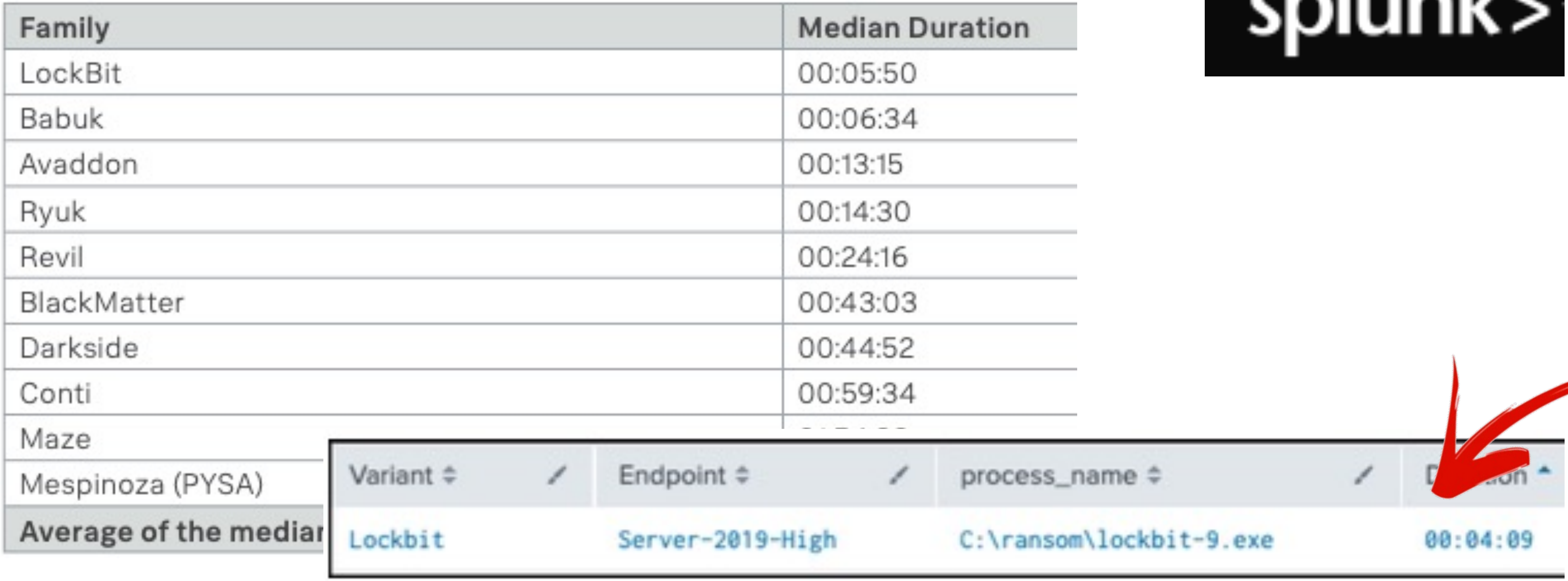
09.20.2022 **FEATURED STORY**

Ripple effects of ransomware attack against Suffolk County continue more than a week later

By Joe Werkmeister

Better, Faster Ransomware

Time to Encrypt 53 GB / ~100,000 test files

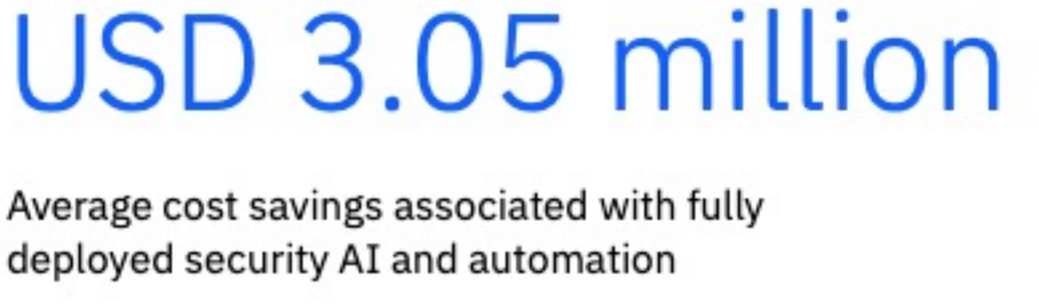


Family	Median Duration
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	[illegible]
Mespinoza (PYSA)	
Average of the median	

Variant	Endpoint	process_name	Duration
Lockbit	Server-2019-High	C:\ransom\lockbit-9.exe	00:04:09

Figure 5. Data from the lockbit-9.exe sample deployed on a Windows 2019 server.

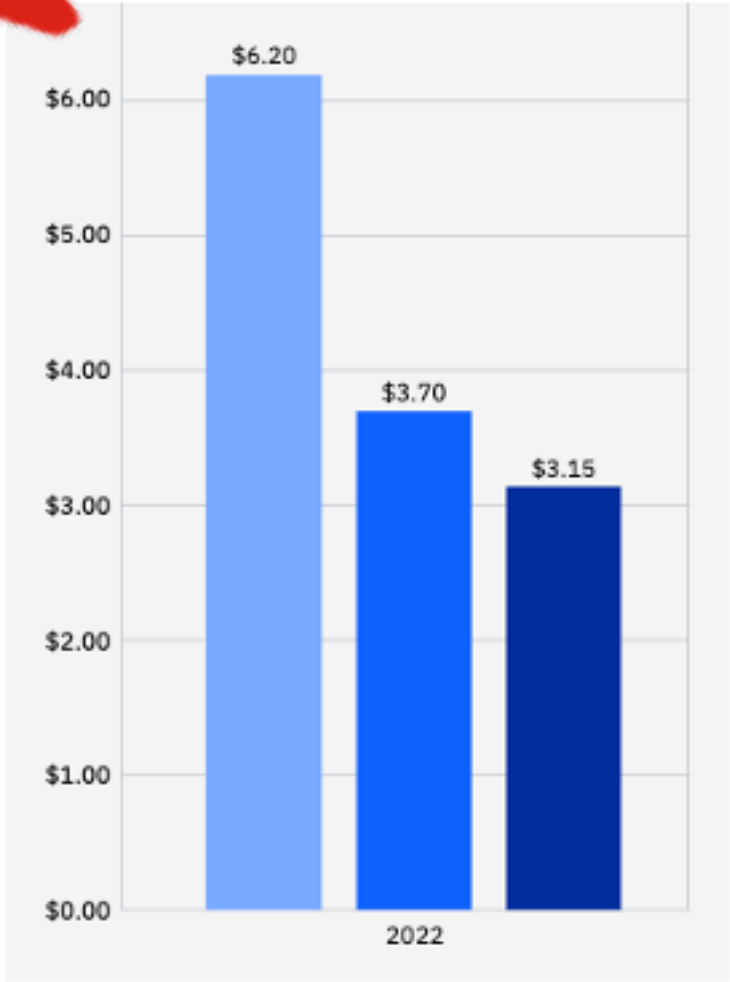
AI/Automation Dramatically Improves Response



USD 3.05 million

Average cost savings associated with fully deployed security AI and automation

> “Organizations with fully deployed security AI and automation were able to detect and contain a breach much more quickly than organizations with no security AI and automation deployed.”



IBM *Cost of a Data Breach 2022*, p. 23

Endpoint Detection and Response (EDR)

FALCON
PRO

Replace legacy AV with market-leading NGAV and integrated threat intelligence and immediate response

$8.99
per endpoint/month*

- Real-time continuous monitoring
- Live response
- Threat hunting
- Historical data collection
- Highly automated

"How is EDR Different from Antivirus?"

EDR

Antivirus ☹

©LMG Security 2021. All rights reserved.

EDR vs Antivirus

- EDR:
  - Integrated threat int
  - Behavioral detectior
  - Quarantine function
  - Forensic informatior
  - Live mitigation capal
  - Often contains antiv

stem scanning

scans

ile removal (sometimes only

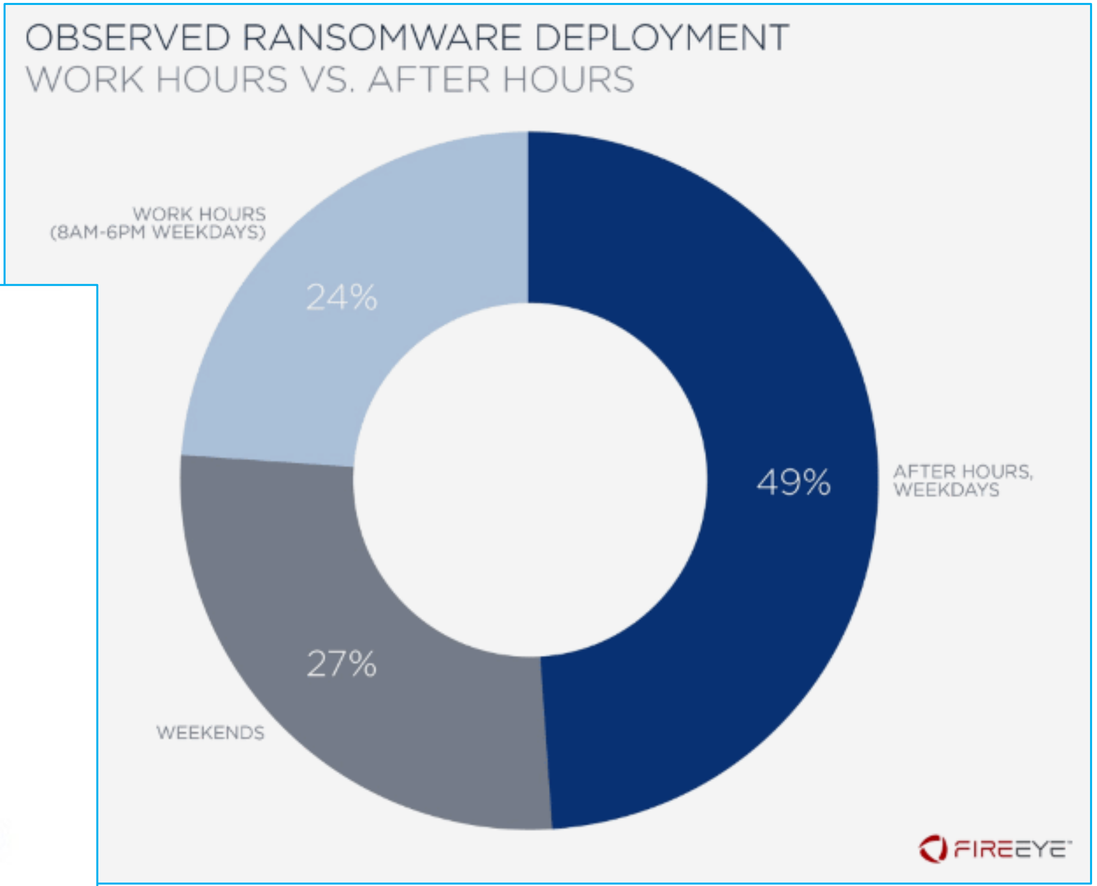
Timing of Ransomware Attacks

- Fourth of July weekend
- Kaseya Ransomware Attacks
  - Coincidence?
  - “Forensics Friday” @LMG
- Locked up w ransomware
- Need a fast, effective response!

In

76%

of cases, ransomware was executed outside work hours



OBSERVED RANSOMWARE DEPLOYMENT
WORK HOURS VS. AFTER HOURS
WORK HOURS (8AM-6PM WEEKDAYS)
24%
49%
AFTER HOURS, WEEKDAYS
27%
WEEKENDS
FIREEYE

https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html

©LMG Security 2021. All rights reserved.

Continuous Security Monitoring

ARCTIC WOLF

Basic Plan: $21K Annually
(300 Assets)

eSENTIRE

Basic Plan: $22K Annually
(300 Assets)

RAPID7

Essential Plan: $17/Asset* per Month
Elite Plan: $23/Asset* per Month
(*300 Asset minimum) $61k – $83K Annually

Conduct Tabletop Exercises

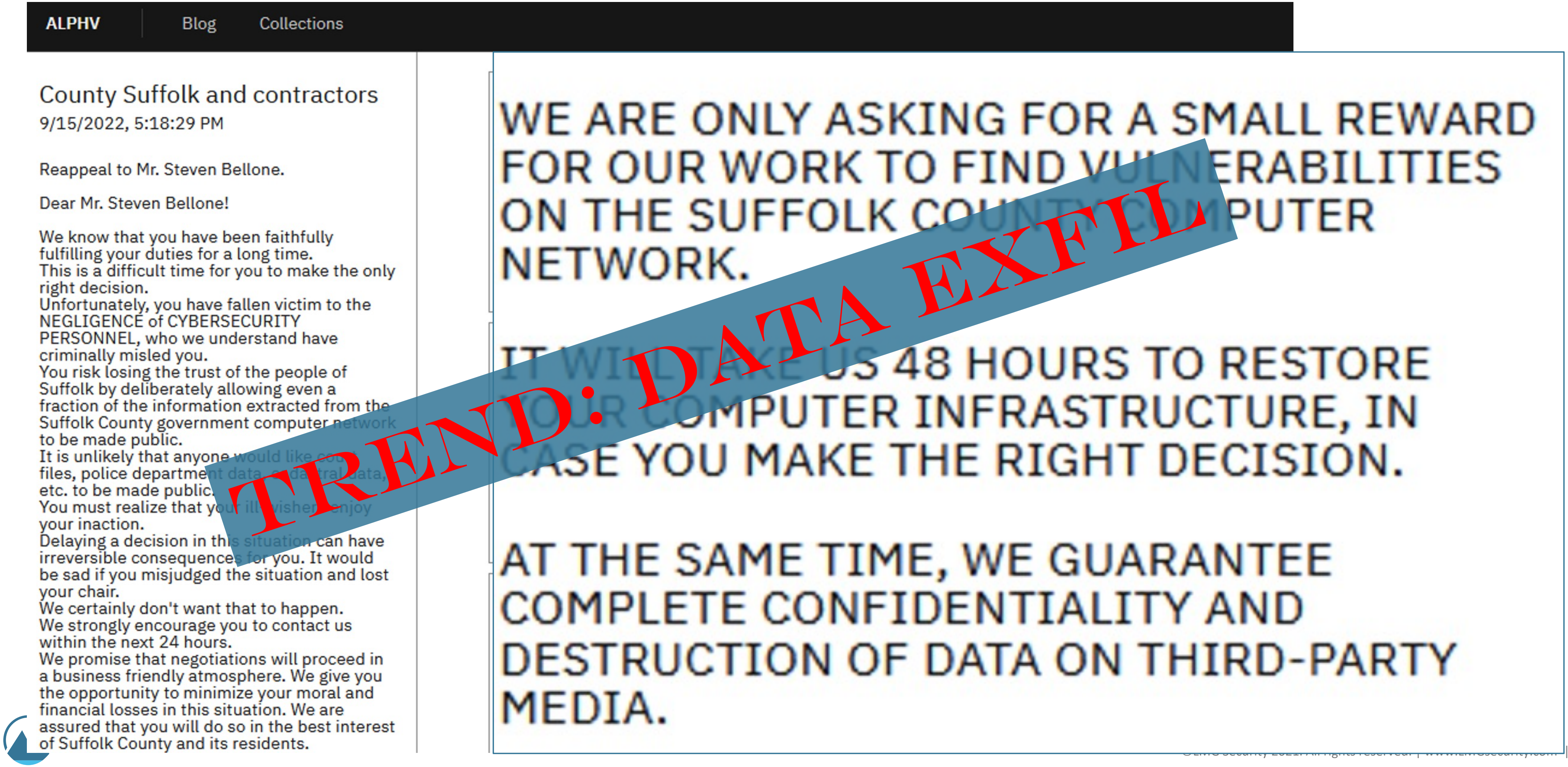
- Live simulated cyber events
  - Ransomware
  - BEC
  - Malware
  - Supply chain attacks & more
- Virtual or onsite
- Test processes, communications, etc.
- Clarify roles & responsibilities
- Align expectations & Identify gaps
- Fun & educational

USD 2.66 million

Average cost savings associated with an incident response (IR) team and regularly tested IR plan

IBM, “Cost of a Data Breach 2022”

Back to the Case: Hackers Stole 4TB+ of Data



County Suffolk and contractors
9/15/2022, 5:18:29 PM

Reappeal to Mr. Steven Bellone.

Dear Mr. Steven Bellone!

We know that you have been faithfully fulfilling your duties for a long time.
This is a difficult time for you to make the only right decision.
Unfortunately, you have fallen victim to the NEGLIGENCE of CYBERSECURITY PERSONNEL, who we understand have criminally misled you.
You risk losing the trust of the people of Suffolk by deliberately allowing even a fraction of the information extracted from the Suffolk County government computer network to be made public.
It is unlikely that anyone would like court files, police department data, cadastral data, etc. to be made public.
You must realize that your ill-wishers enjoy your inaction.
Delaying a decision in this situation can have irreversible consequences for you. It would be sad if you misjudged the situation and lost your chair.
We certainly don't want that to happen.
We strongly encourage you to contact us within the next 24 hours.
We promise that negotiations will proceed in a business friendly atmosphere. We give you the opportunity to minimize your moral and financial losses in this situation. We are assured that you will do so in the best interest of Suffolk County and its residents.

WE ARE ONLY ASKING FOR A SMALL REWARD FOR OUR WORK TO FIND VULNERABILITIES ON THE SUFFOLK COUNTY COMPUTER NETWORK.

IT WILL TAKE US 48 HOURS TO RESTORE YOUR COMPUTER INFRASTRUCTURE, IN CASE YOU MAKE THE RIGHT DECISION.

AT THE SAME TIME, WE GUARANTEE COMPLETE CONFIDENTIALITY AND DESTRUCTION OF DATA ON THIRD-PARTY MEDIA.

TREND: DATA EXFIL

More Data = Higher Damages When it Leaks

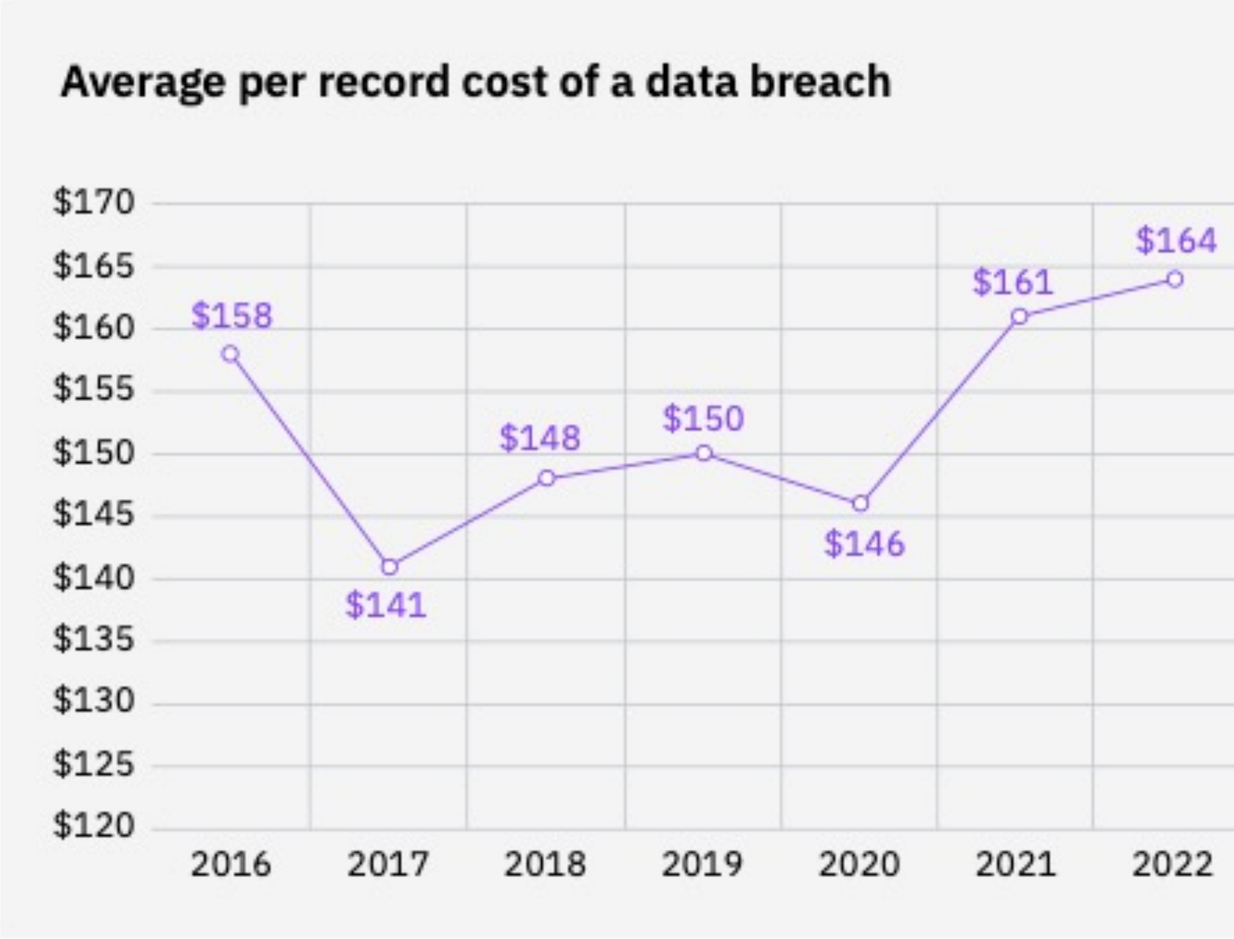
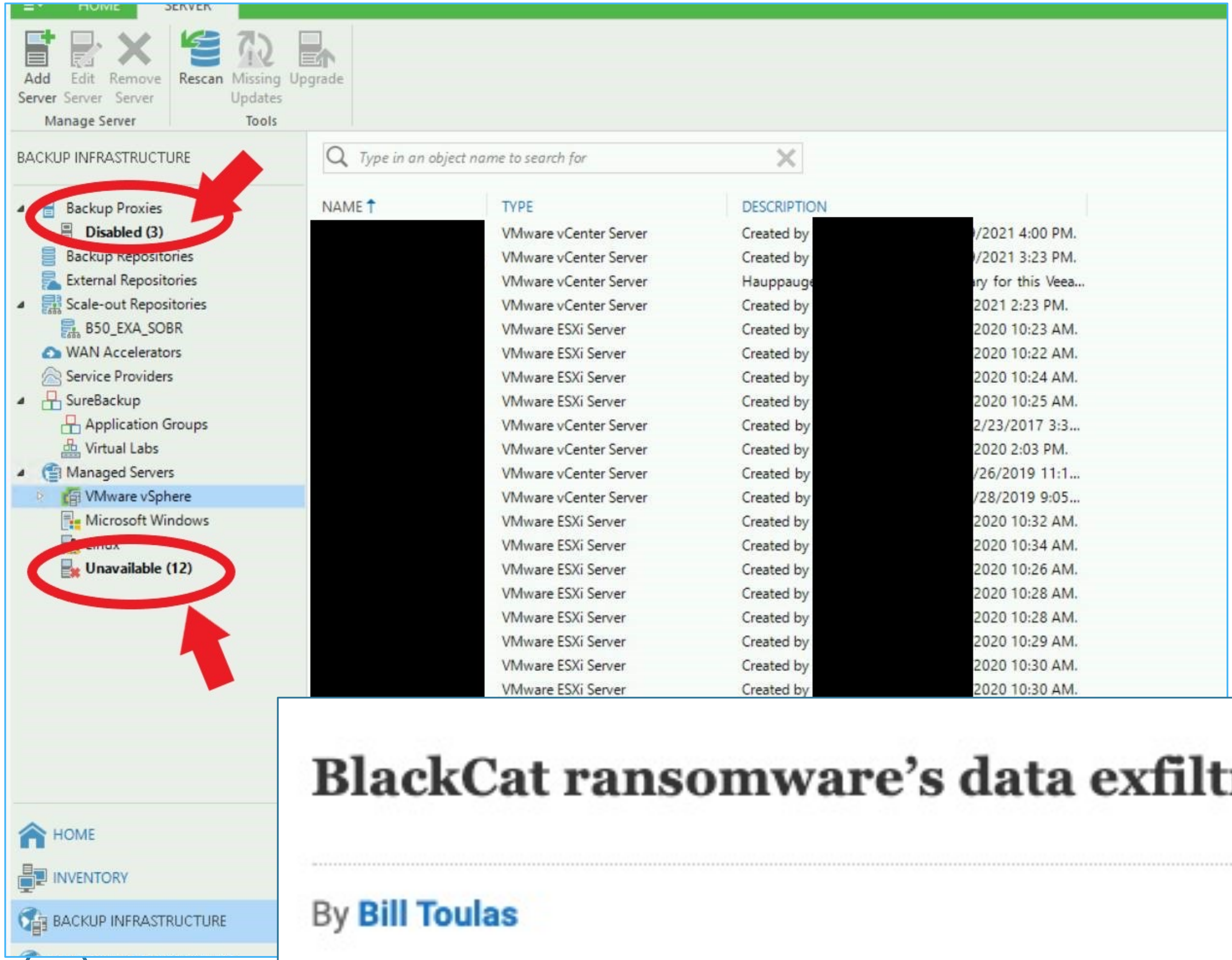


Figure 2: Measured in USD

Attacking Backups…



NAME ↑	TYPE	DESCRIPTION
[redacted]	VMware vCenter Server	Created by [redacted] /2021 4:00 PM.
[redacted]	VMware vCenter Server	Created by [redacted] /2021 3:23 PM.
[redacted]	VMware vCenter Server	Hauppauge [redacted] ry for this Veea...
[redacted]	VMware vCenter Server	Created by [redacted] 2021 2:23 PM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:23 AM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:22 AM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:24 AM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:25 AM.
[redacted]	VMware vCenter Server	Created by [redacted] 2/23/2017 3:3...
[redacted]	VMware vCenter Server	Created by [redacted] 2020 2:03 PM.
[redacted]	VMware vCenter Server	Created by [redacted] /26/2019 11:1...
[redacted]	VMware vCenter Server	Created by [redacted] /28/2019 9:05...
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:32 AM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:34 AM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:26 AM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:28 AM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:28 AM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:29 AM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:30 AM.
[redacted]	VMware ESXi Server	Created by [redacted] 2020 10:30 AM.

Noberus Ransomware: Darkside and BlackMatter Successor Continues to Evolve its Tactics

New version of Exmatter, and Eamfo malware, used by attackers deploying the Rust-based ransomware.

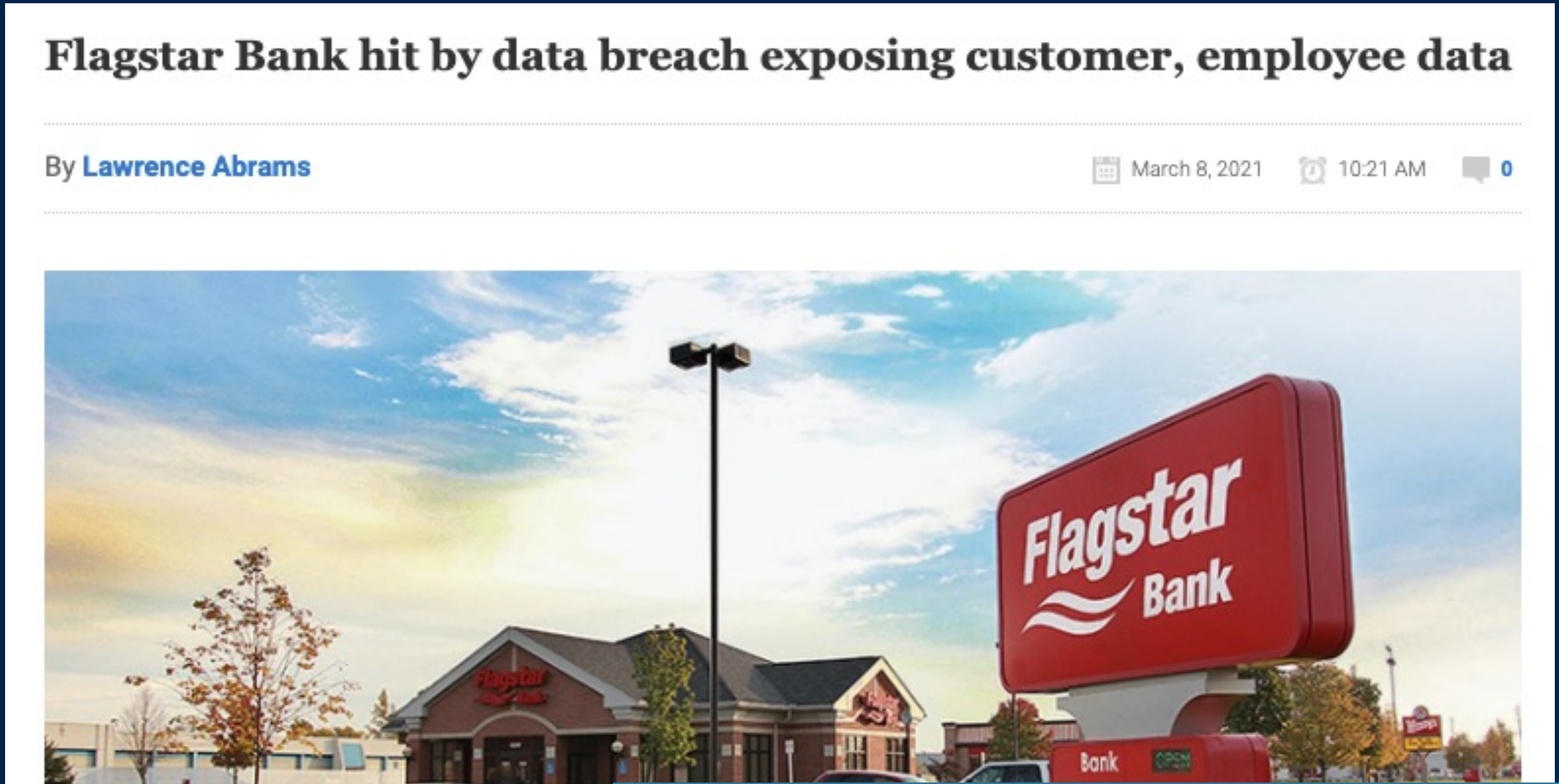
BlackCat ransomware's data exfiltration tool gets an upgrade

By Bill Toulas September 22, 2022 06:00 AM 0

Maintain and Test Your Backups

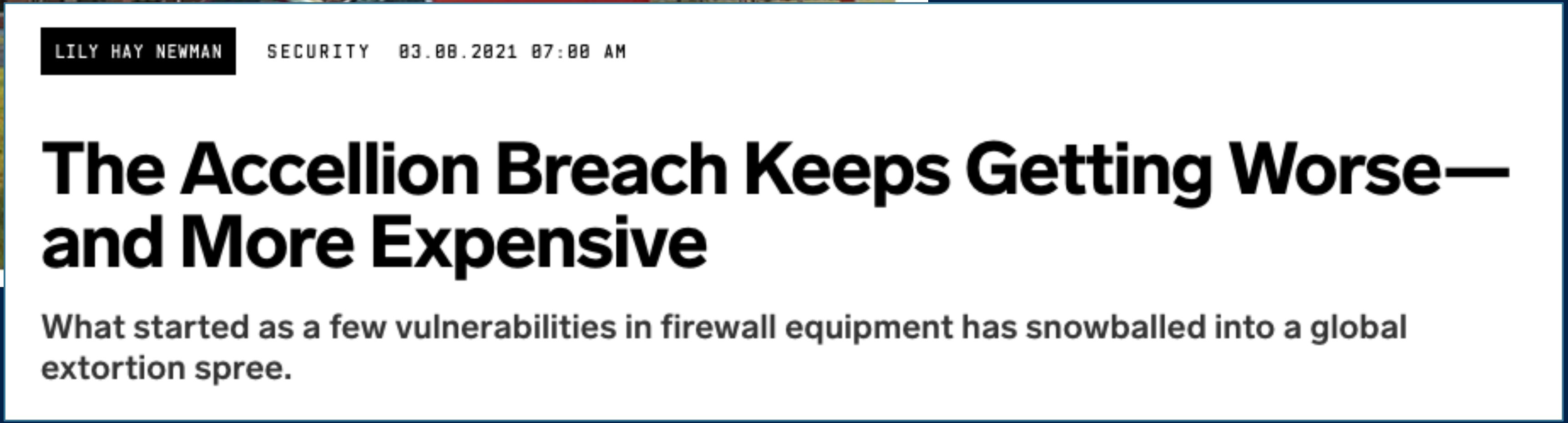
- Archive, encrypt and store data offsite
- Immutable
- Encrypted
- Retention times
- VM environment
- Plan for restoration time
- Include Cloud Apps
- Test your backups!
  - Or you don't have backups

Configuration matters!



Flagstar Bank hit by data breach exposing customer, employee data

By Lawrence Abrams March 8, 2021 10:21 AM 0

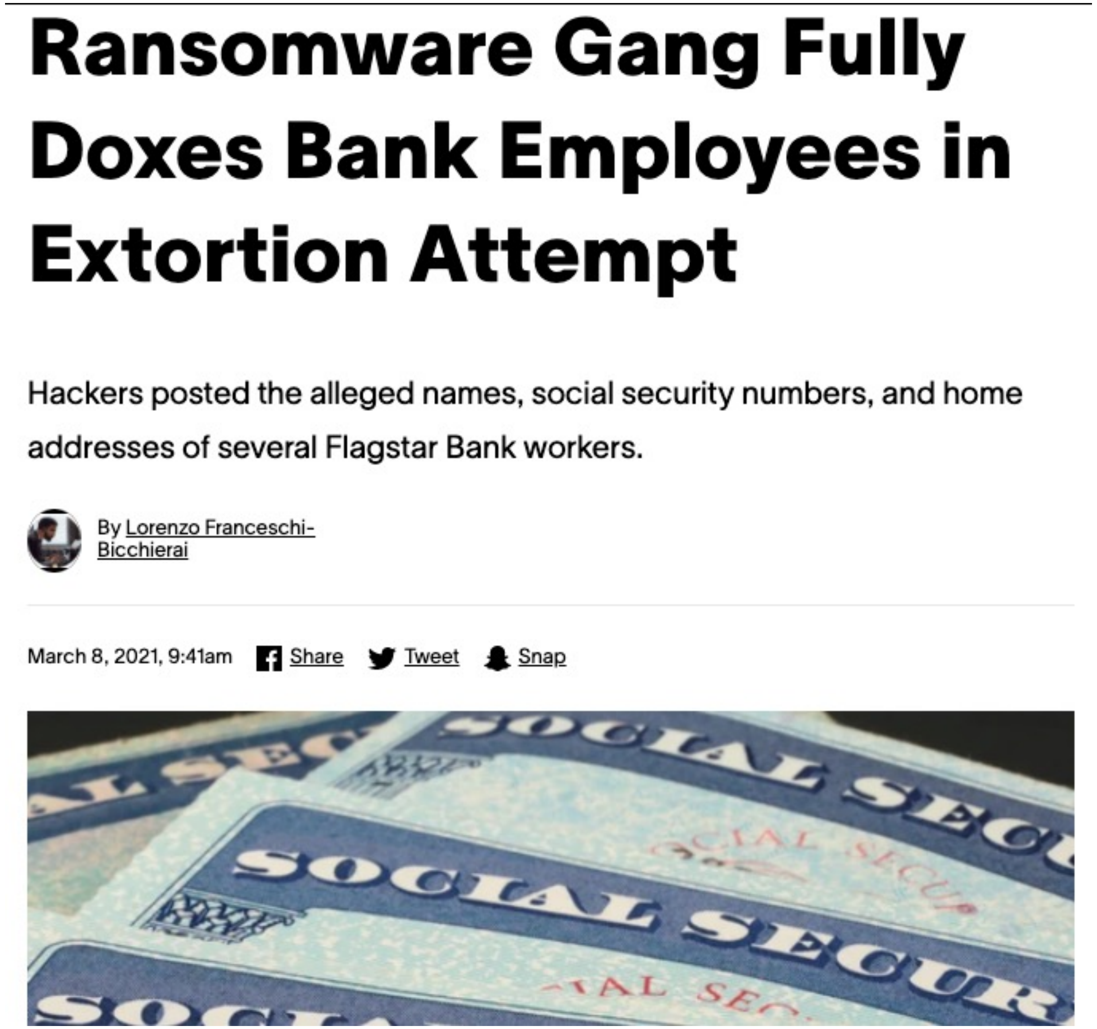


LILY HAY NEWMAN SECURITY 03.08.2021 07:00 AM

The Accellion Breach Keeps Getting Worse—and More Expensive

What started as a few vulnerabilities in firewall equipment has snowballed into a global extortion spree.

But Wait, It Gets Worse…



Ransomware Gang Fully Doxes Bank Employees in Extortion Attempt

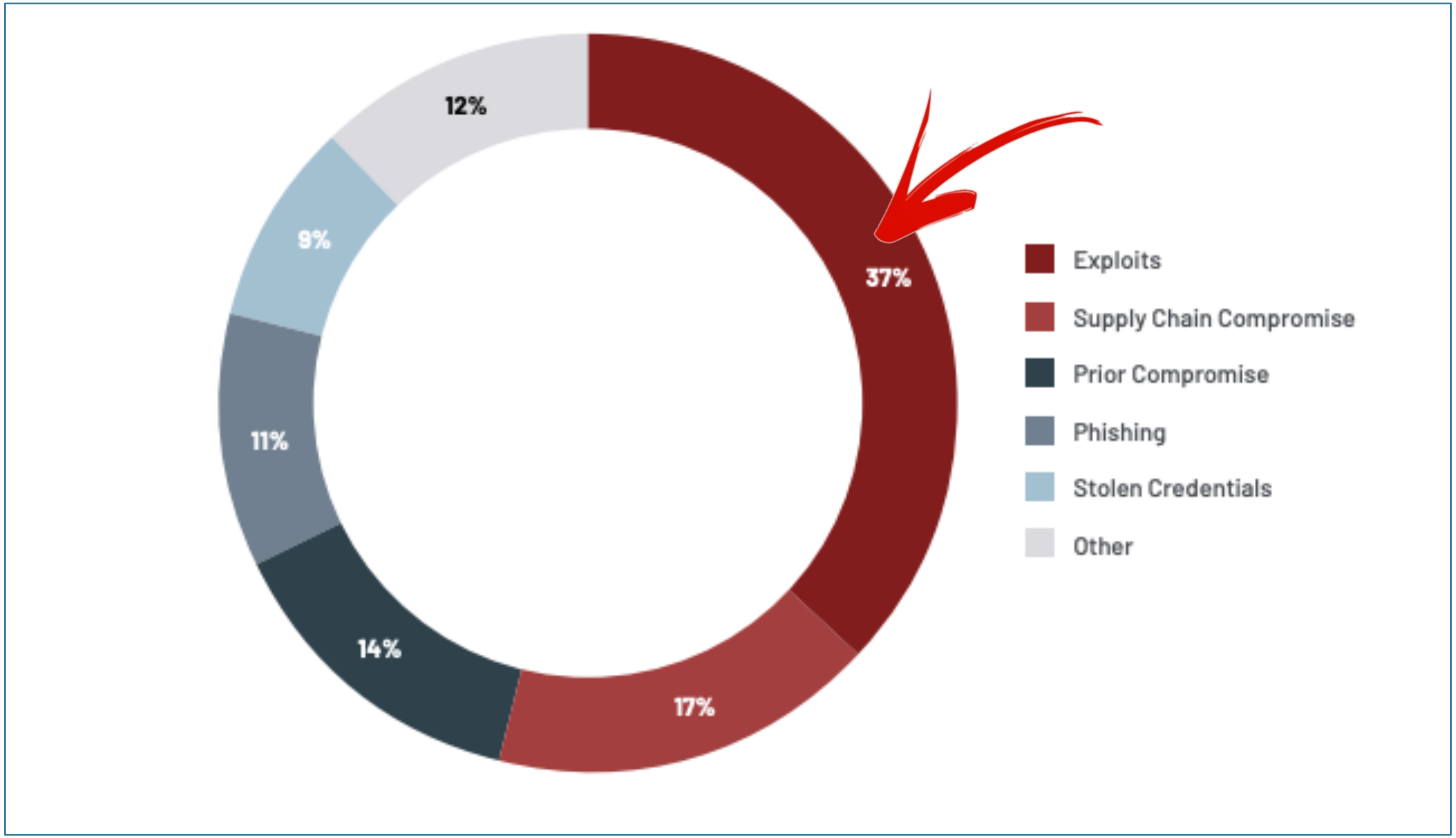
Hackers posted the alleged names, social security numbers, and home addresses of several Flagstar Bank workers.

By Lorenzo Franceschi-Bicchierai

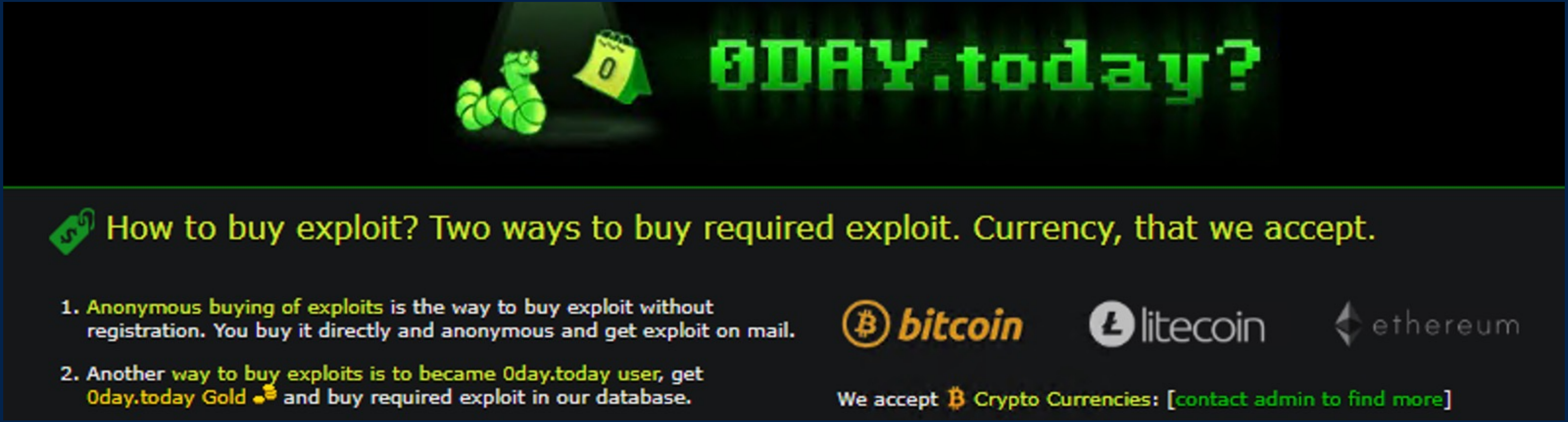
March 8, 2021, 9:41am Share Tweet Snap

"On Monday, the hacking group known as Cl0p published the data from Flagstar Bank on a dark web site, and emailed reporters to advertise the extortion attempt. The hackers said that they published the data hoping to convince the bank to pay them to stop leaking its internal data." – Vice Magazine

Threat: Software Exploits



https://www.mandiant.com/sites/default/files/2022-04/M-Trends%202022%20Executive%20Summary.pdf

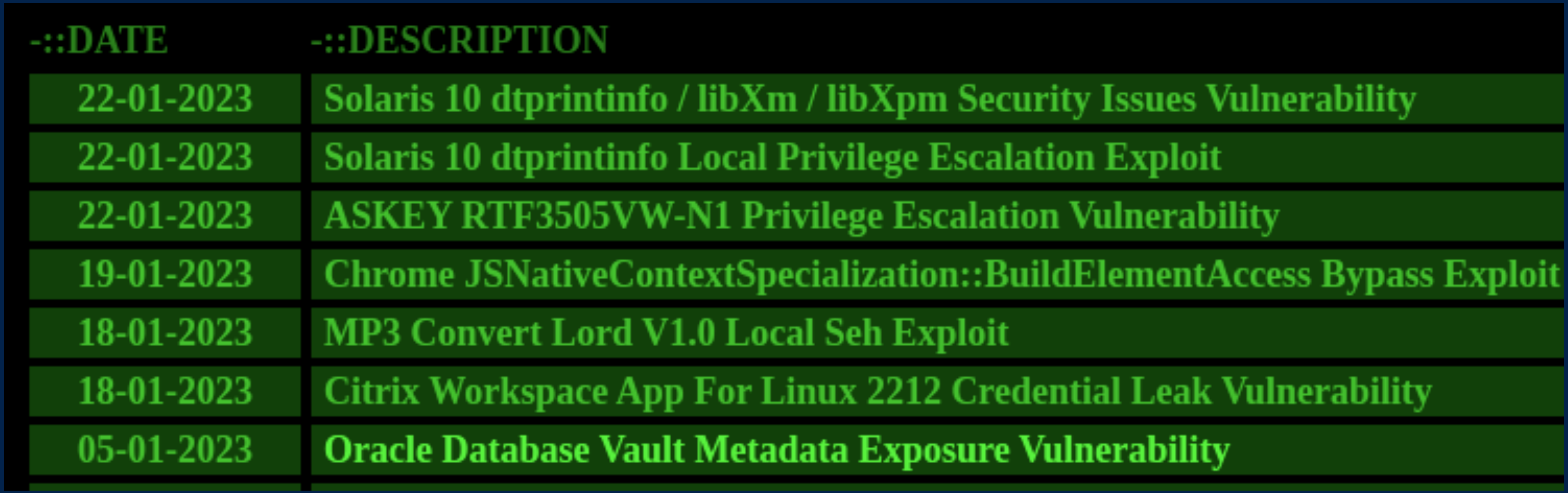


0DAY.today?

How to buy exploit? Two ways to buy required exploit. Currency, that we accept.

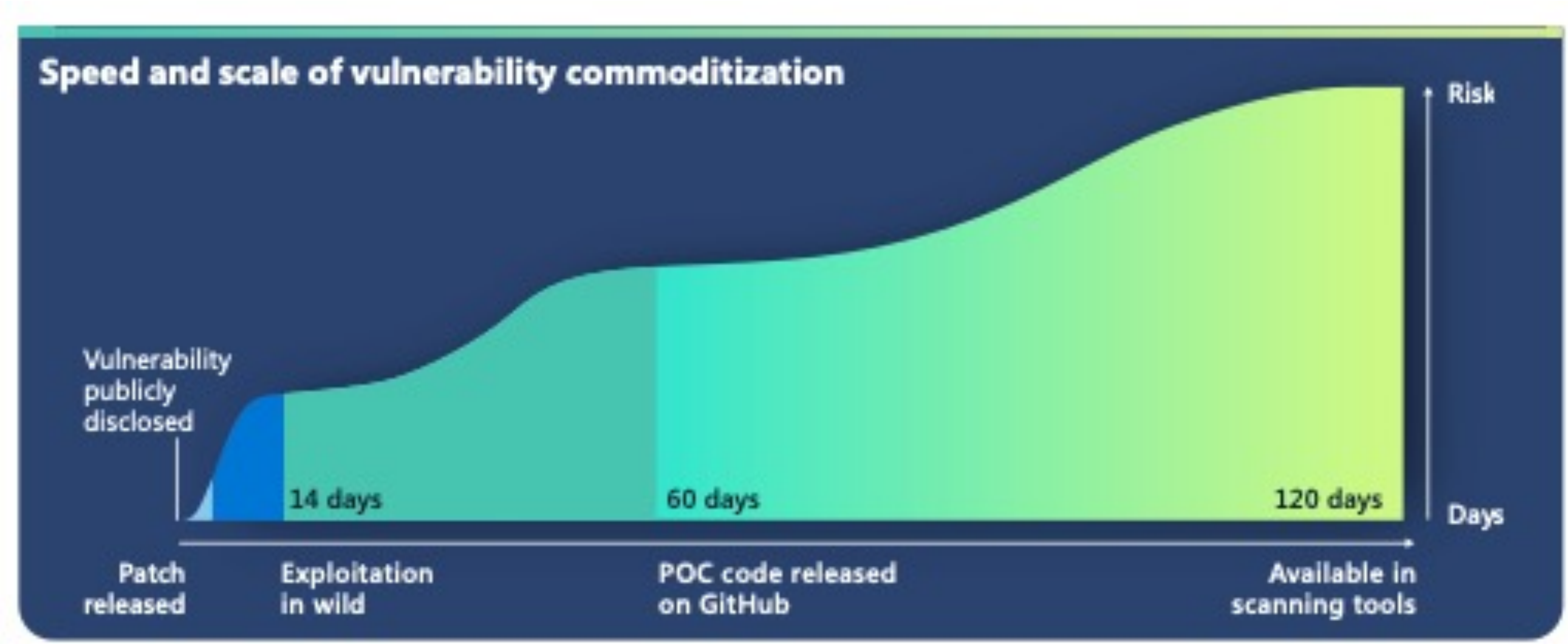
1. Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
2. Another way to buy exploits is to became 0day.today user, get 0day.today Gold and buy required exploit in our database.

We accept ₿ Crypto Currencies: [contact admin to find more]



-::DATE	-::DESCRIPTION
22-01-2023	Solaris 10 dtprintinfo / libXm / libXpm Security Issues Vulnerability
22-01-2023	Solaris 10 dtprintinfo Local Privilege Escalation Exploit
22-01-2023	ASKEY RTF3505VW-N1 Privilege Escalation Vulnerability
19-01-2023	Chrome JSNativeContextSpecialization::BuildElementAccess Bypass Exploit
18-01-2023	MP3 Convert Lord V1.0 Local Seh Exploit
18-01-2023	Citrix Workspace App For Linux 2212 Credential Leak Vulnerability
05-01-2023	Oracle Database Vault Metadata Exposure Vulnerability

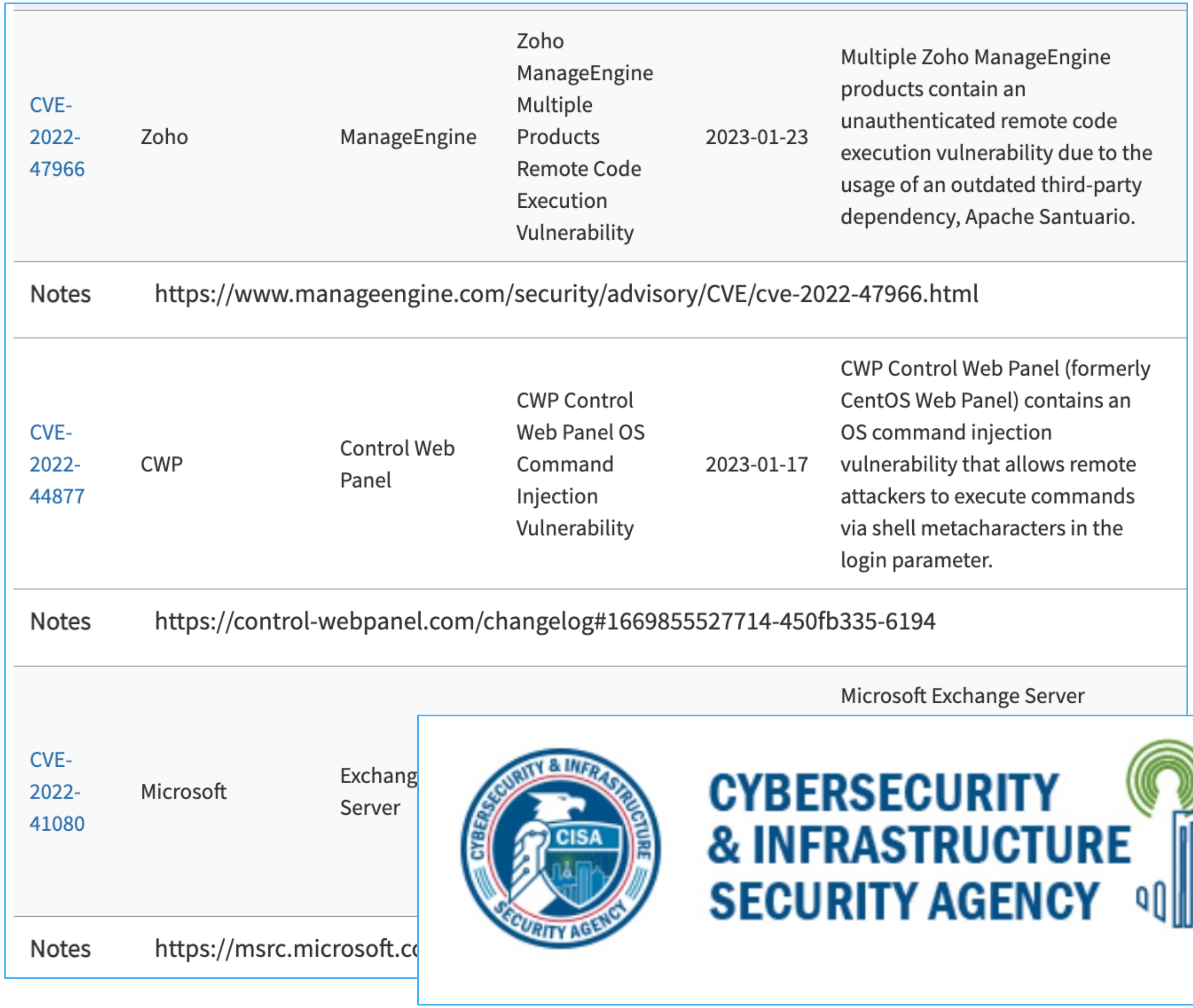
Rapid Exploitation of Zero-Day Vulnerabilities



Microsoft Digital Defense Report: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

Monitor Your Attack Surface

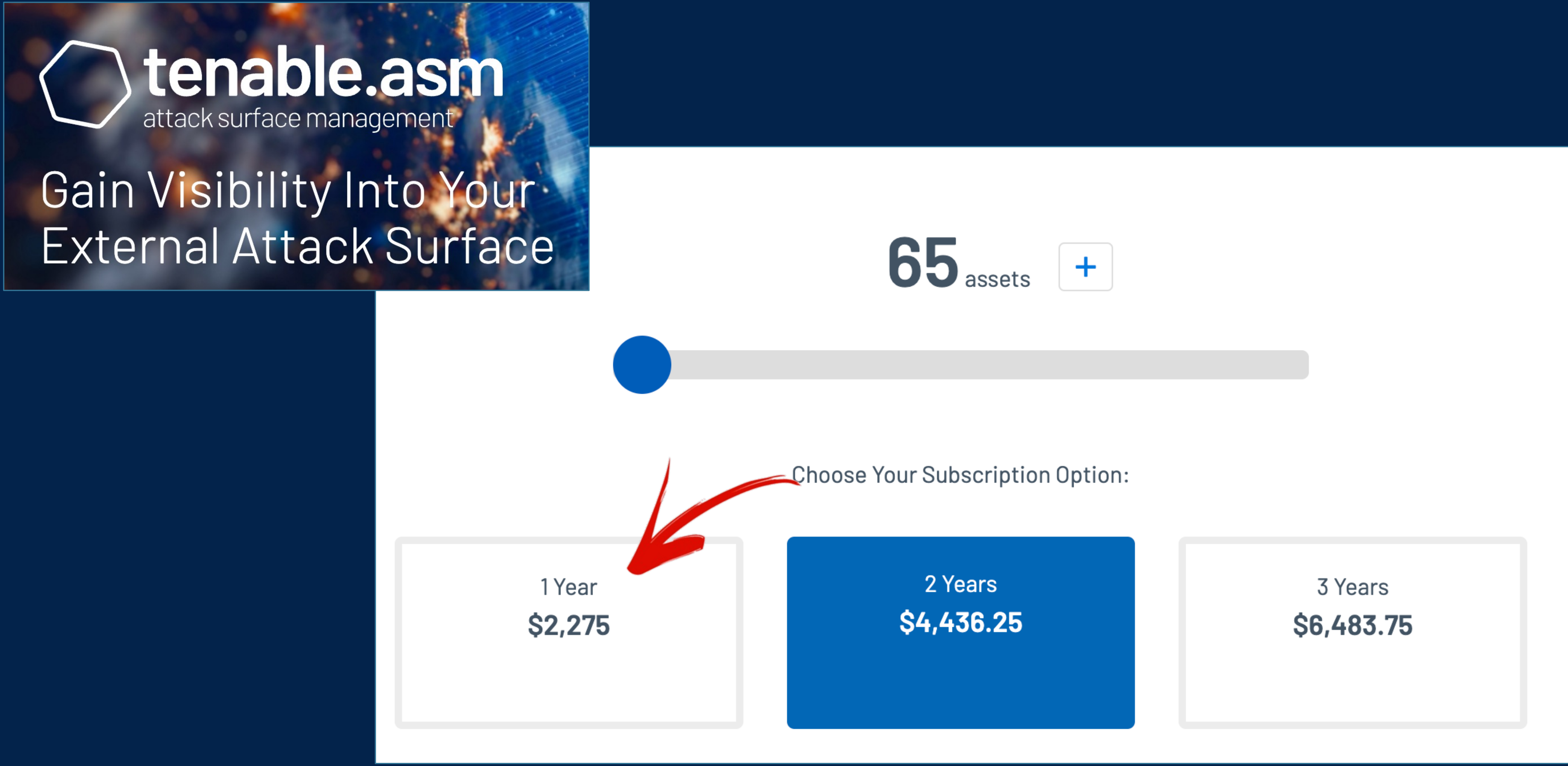
- Verify patching
- Audit configurations
- Scan the external facing parts of the network
- Include your cloud!



CVE-2022-47966	Zoho	ManageEngine	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	2023-01-23	Multiple Zoho ManageEngine products contain an unauthenticated remote code execution vulnerability due to the usage of an outdated third-party dependency, Apache Santuario.
Notes	https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html				
CVE-2022-44877	CWP	Control Web Panel	CWP Control Web Panel OS Command Injection Vulnerability	2023-01-17	CWP Control Web Panel (formerly CentOS Web Panel) contains an OS command injection vulnerability that allows remote attackers to execute commands via shell metacharacters in the login parameter.
Notes	https://control-webpanel.com/changelog#1669855527714-450fb335-6194				
CVE-2022-41080	Microsoft	Exchang Server			Microsoft Exchange Server
Notes	https://msrc.microsoft.c				

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/known-exploited-vulnerabilities-catalog


tenable.asm
attack surface management
Gain Visibility Into Your External Attack Surface

65 assets +

Choose Your Subscription Option:

1 Year
$2,275

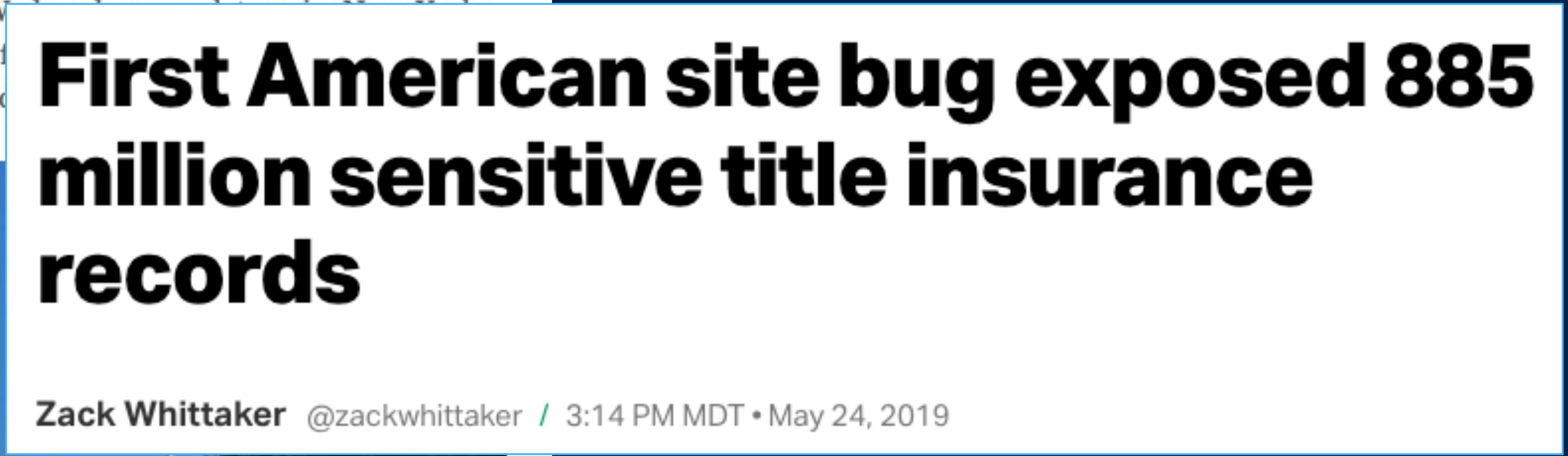
2 Years
$4,436.25

3 Years
$6,483.75

23 JUL 20 NY Charges First American Financial for Massive Data Leak

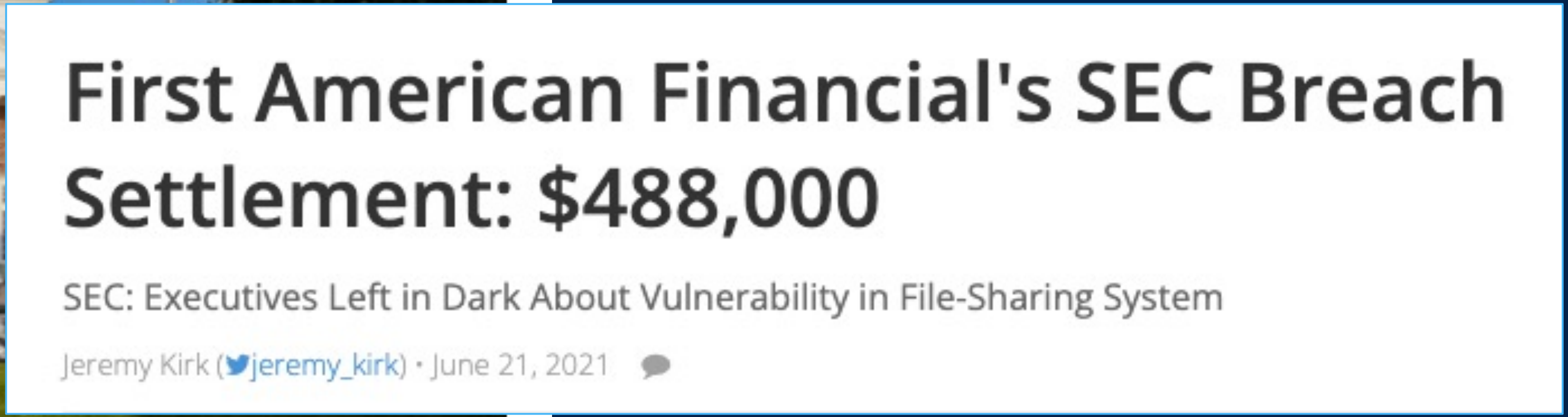
In May 2019, KrebsOnSecurity broke the news that the website of mortgage title insurance giant **First American Financial Corp.** had exposed approximately 885 million records related to mortgage deals going back to 2003. On W
announced that First American was the target of their f
action in connection with the incident, charges that could

First American Financial Corp.



First American site bug exposed 885 million sensitive title insurance records

Zack Whittaker @zackwhittaker / 3:14 PM MDT • May 24, 2019



First American Financial's SEC Breach Settlement: $488,000

SEC: Executives Left in Dark About Vulnerability in File-Sharing System

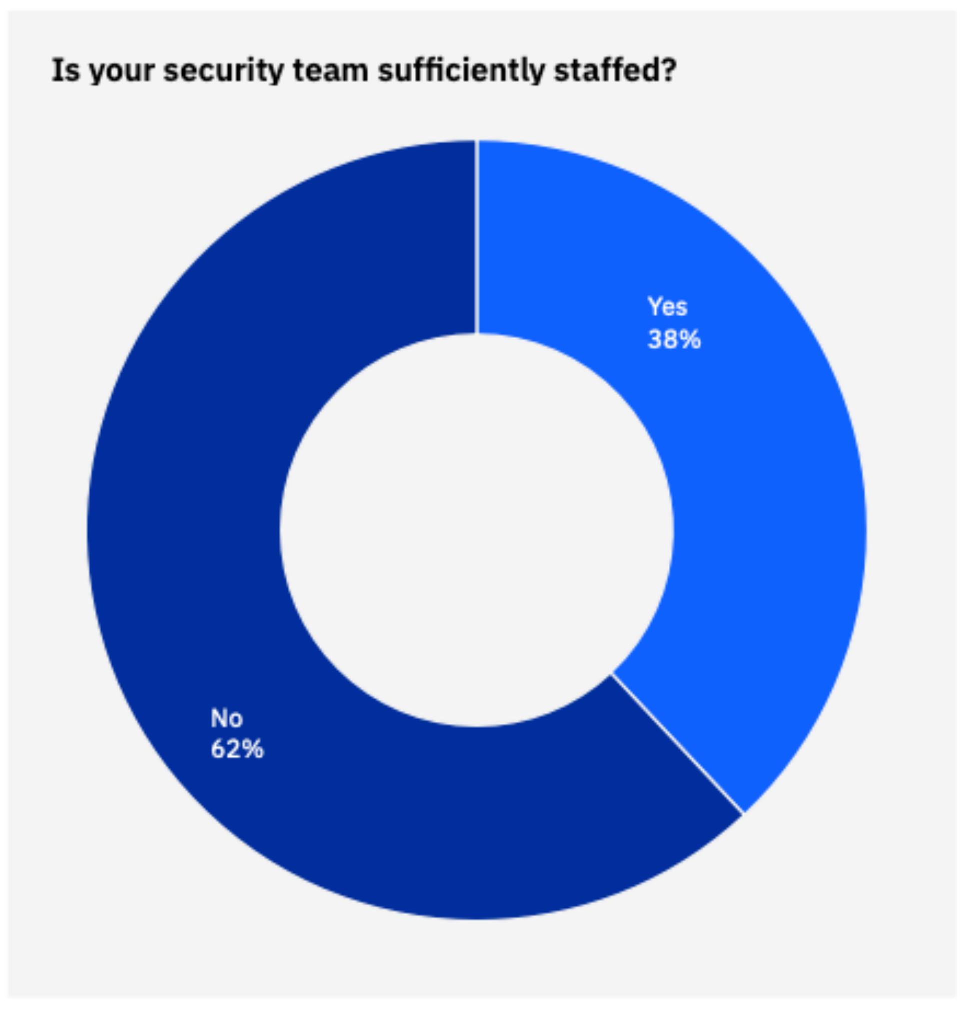
Jeremy Kirk (jeremy_kirk) • June 21, 2021

Conduct Penetration Testing

- Ethical hackers find your weaknesses before the bad guys
- Get an accurate understanding of your risk
- Identify fundamental issues that automated scans won’t detect
- Get to the root of cybersecurity weaknesses
- Demonstrate the risk
- Prioritize cybersecurity investments effectively

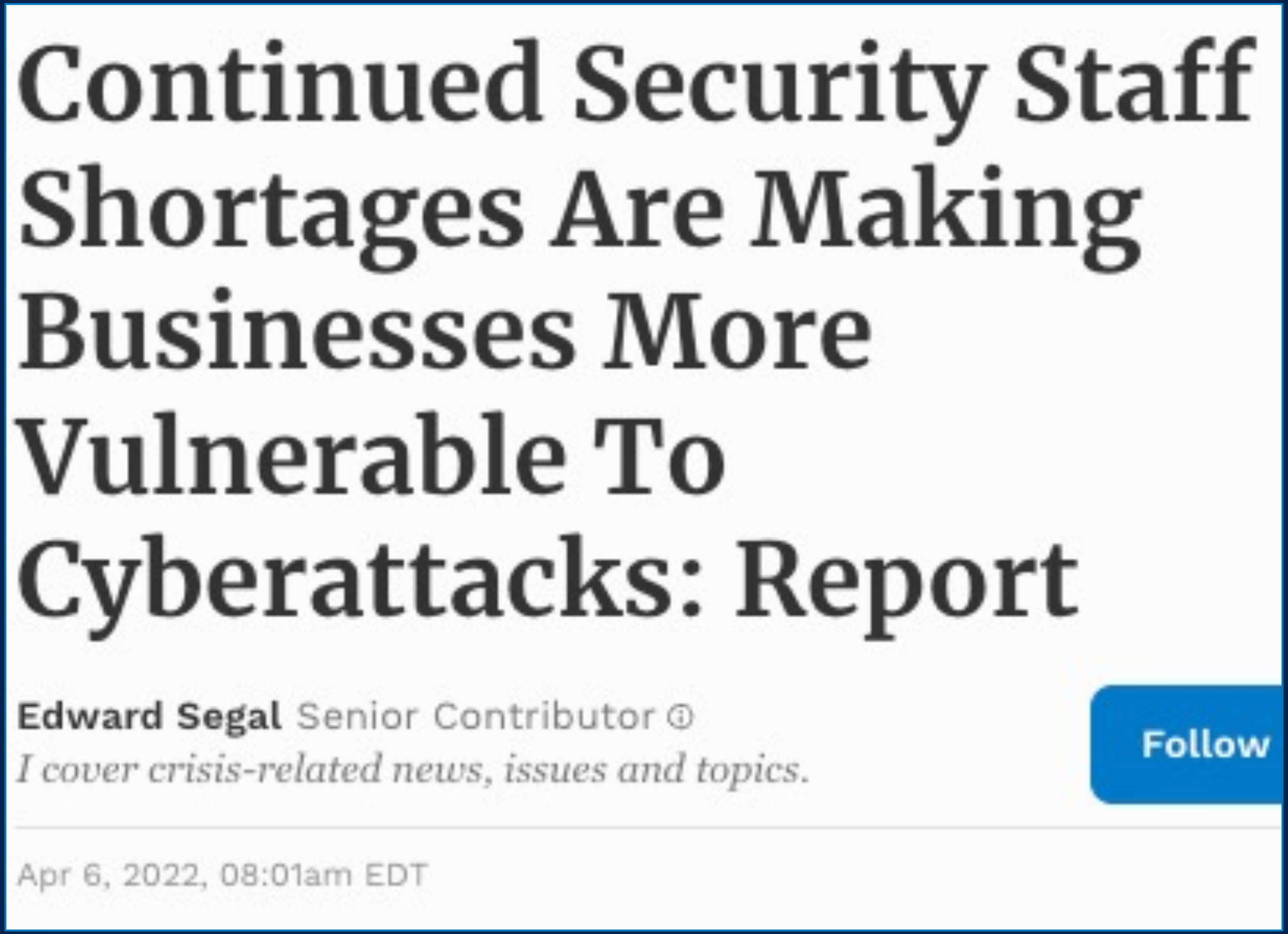
Effective Patch Management

- Takes time & manpower
- Operating system & 3rd party apps
- Requires application inventory & tracking



Is your security team sufficiently staffed?

Figure 51



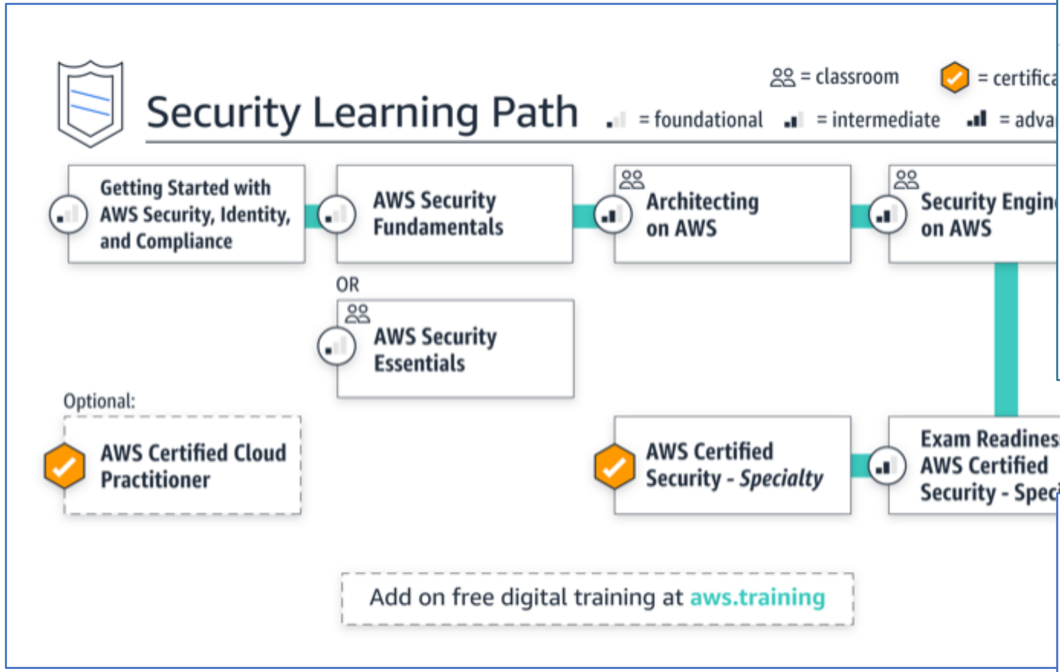
Continued Security Staff Shortages Are Making Businesses More Vulnerable To Cyberattacks: Report

Edward Segal Senior Contributor

I cover crisis-related news, issues and topics.

Apr 6, 2022, 08:01am EDT

Practical, Low-Cost Security Training



Security Learning Path

= classroom · = certifica · = foundational · = intermediate · = adva

Getting Started with AWS Security, Identity, and Compliance

AWS Security Fundamentals

OR

AWS Security Essentials

Architecting on AWS

Security Engin on AWS

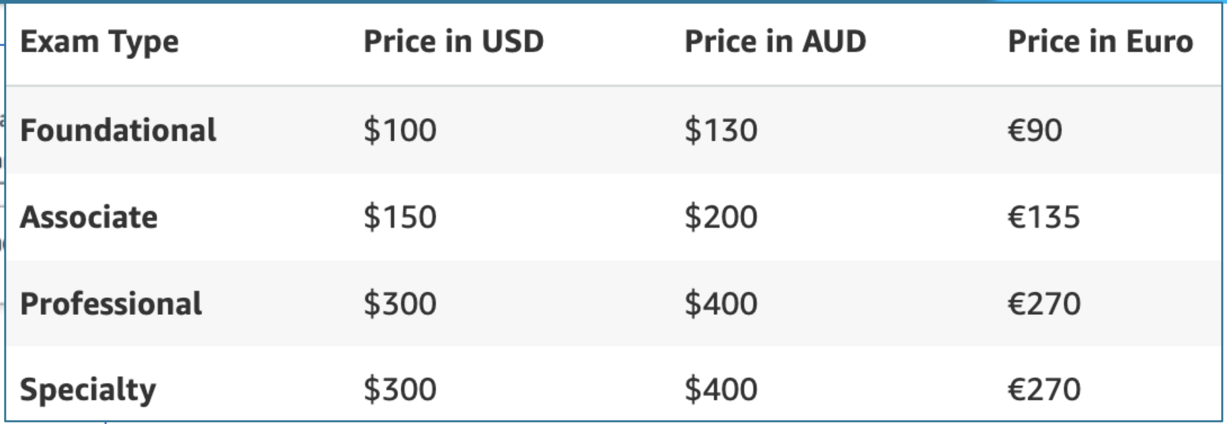
Exam Readiness: AWS Certified Security - Specialty

AWS Certified Security - *Specialty*

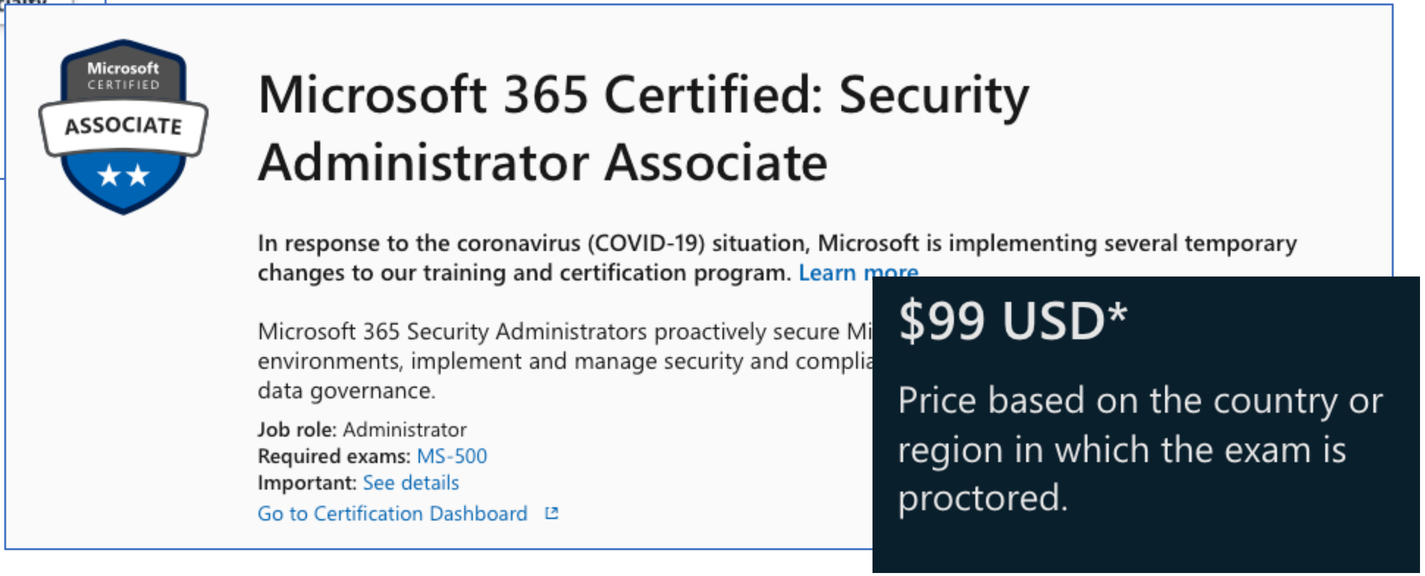
Optional:

AWS Certified Cloud Practitioner

Add on free digital training at aws.training



Exam Type	Price in USD	Price in AUD	Price in Euro
Foundational	$100	$130	€90
Associate	$150	$200	€135
Professional	$300	$400	€270
Specialty	$300	$400	€270



Microsoft 365 Certified: Security Administrator Associate

In response to the coronavirus (COVID-19) situation, Microsoft is implementing several temporary changes to our training and certification program. Learn more

Microsoft 365 Security Administrators proactively secure Mi environments, implement and manage security and complia data governance.

Job role: Administrator
Required exams: MS-500
Important: See details
Go to Certification Dashboard

$99 USD*

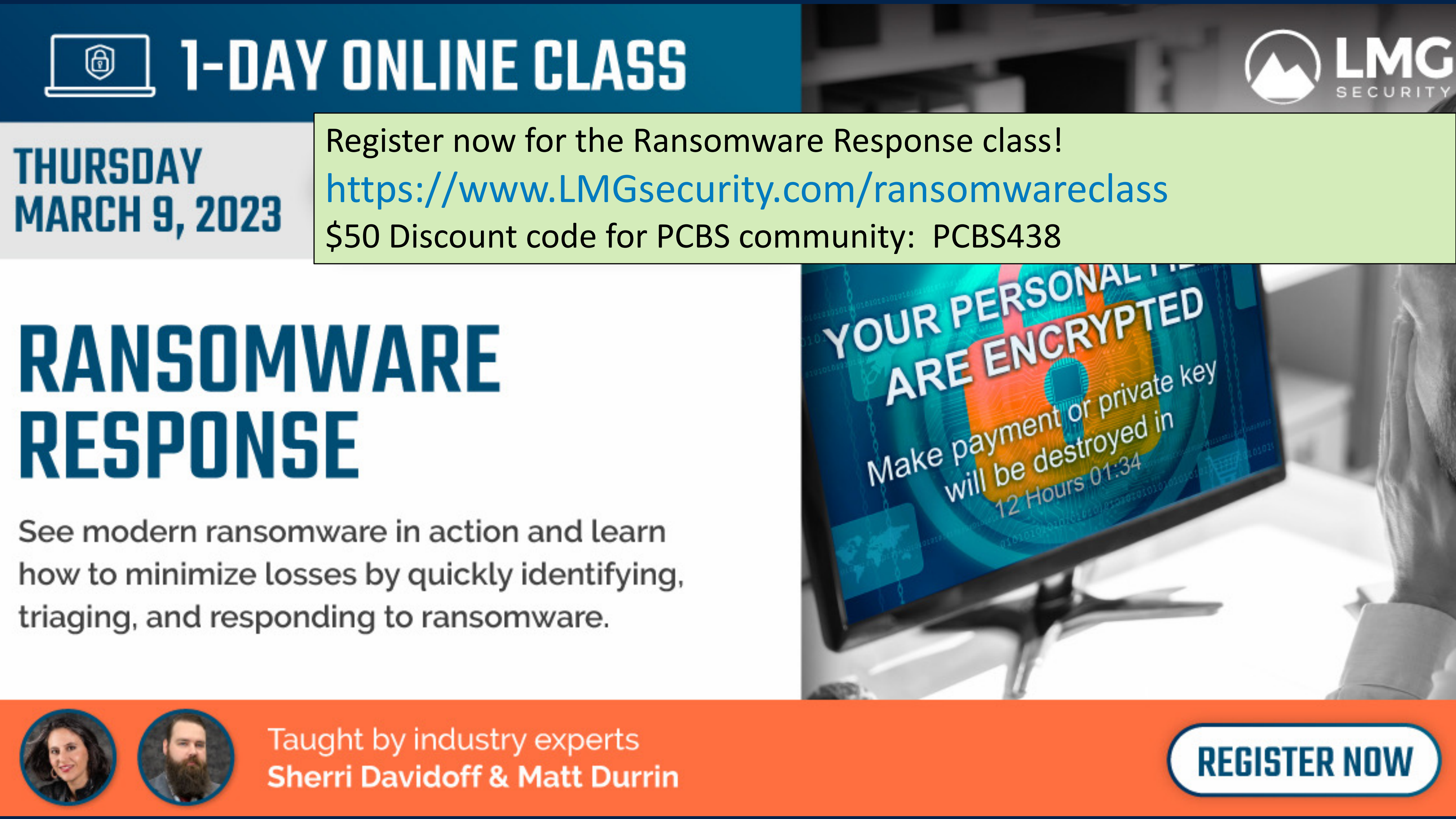
Price based on the country or region in which the exam is proctored.

Training content may be free!

Register now for the Ransomware Response class!

https://www.LMGsecurity.com/ransomwareclass

$50 Discount code for PCBS community: PCBS438



1-DAY ONLINE CLASS

LMG SECURITY

THURSDAY
MARCH 9, 2023

RANSOMWARE RESPONSE

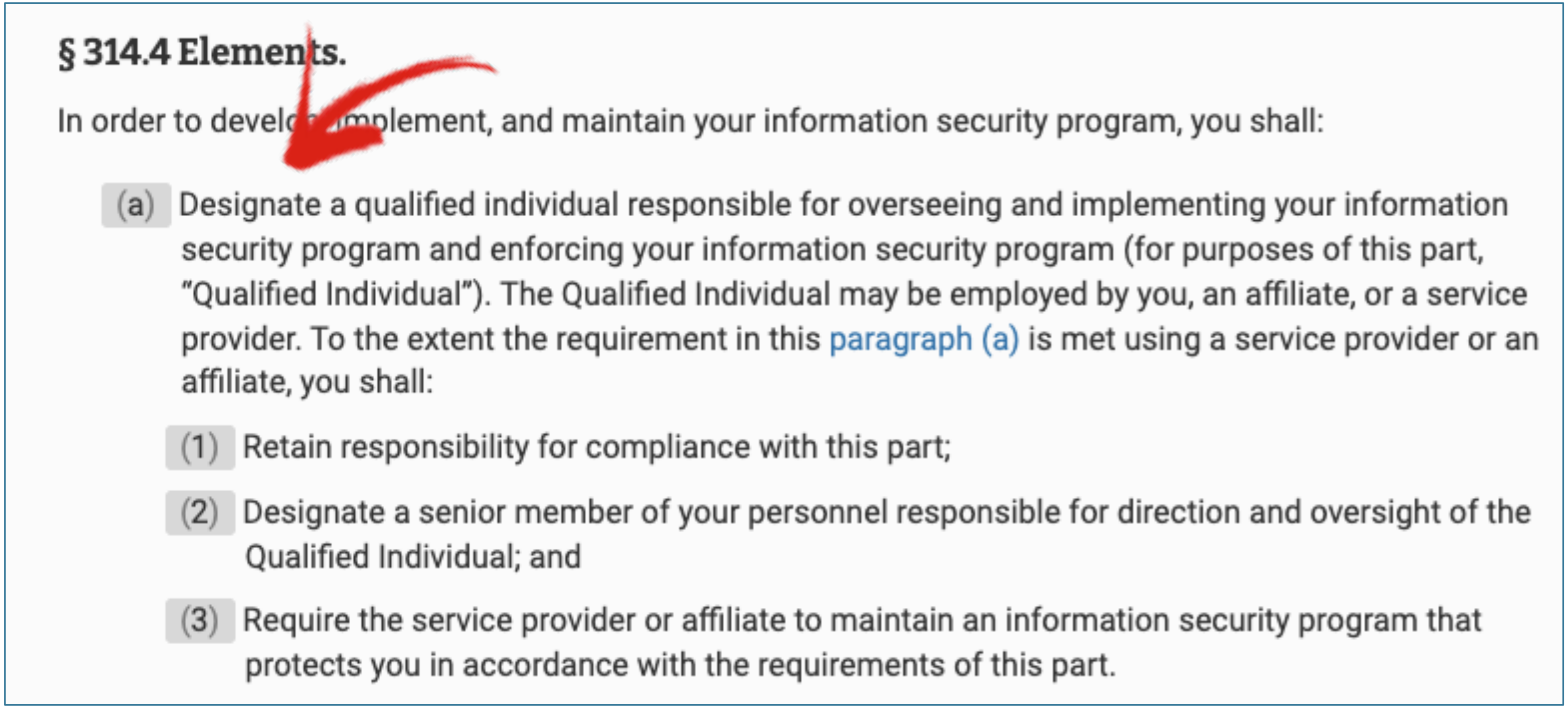
See modern ransomware in action and learn how to minimize losses by quickly identifying, triaging, and responding to ransomware.

Taught by industry experts
Sherri Davidoff & Matt Durrin

REGISTER NOW

New Compliance/Contractual Requirements

Example: GLBA



§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:

(1) Retain responsibility for compliance with this part;

(2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and

(3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

Cybersecurity Starts with Strong Leadership!

"How a security program is planned, executed, and governed is likely as important as how much money is devoted to cybersecurity."

https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/financial-services/DI_Pursuing-cybersecurity-maturity-at-financial-institutions.pdf

Qualified Cybersecurity Leadership

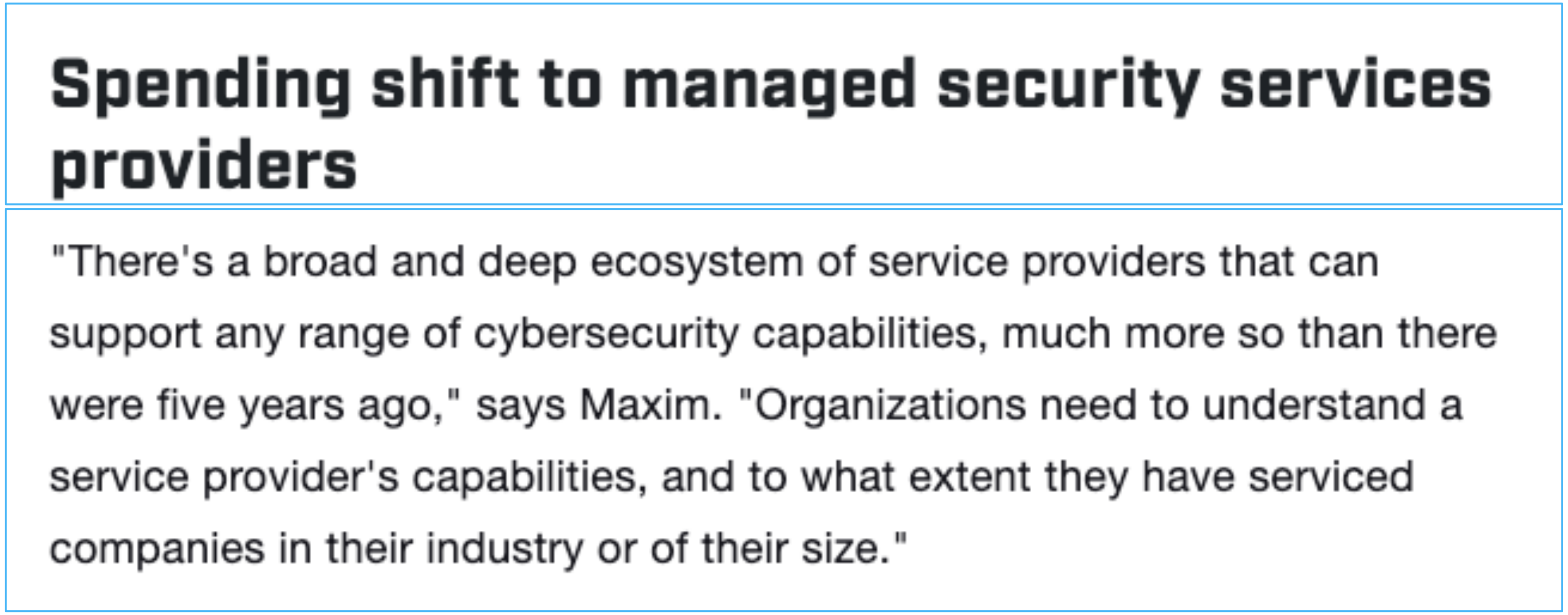
- Every Organization Needs a Qualified CISO or equivalent
- Skills required
  - Cybersecurity experience (not just certificates)
  - Familiarity with Controls Frameworks, Risk Assessments, and Technical Testing
  - Strong IT background as well
- Reduces average cost of a breach by $144,915
- Does not need to be full time
  - You can become a fractional CISO!

Chief Information Security Officer

©LMG Security 2021. All rights reserved.

Outsource Cybersecurity As Needed

- MSSPs
- Cybersecurity projects
- Specialized skills



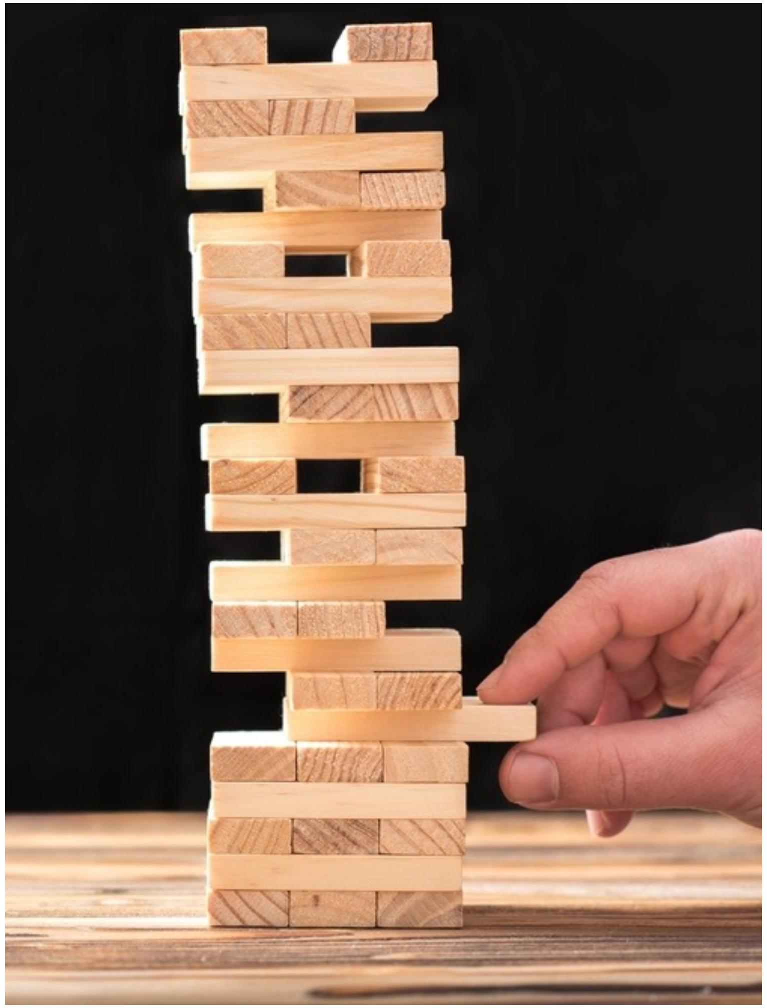
Spending shift to managed security services providers

"There's a broad and deep ecosystem of service providers that can support any range of cybersecurity capabilities, much more so than there were five years ago," says Maxim. "Organizations need to understand a service provider's capabilities, and to what extent they have serviced companies in their industry or of their size."

CSO

Risk Treatment Options

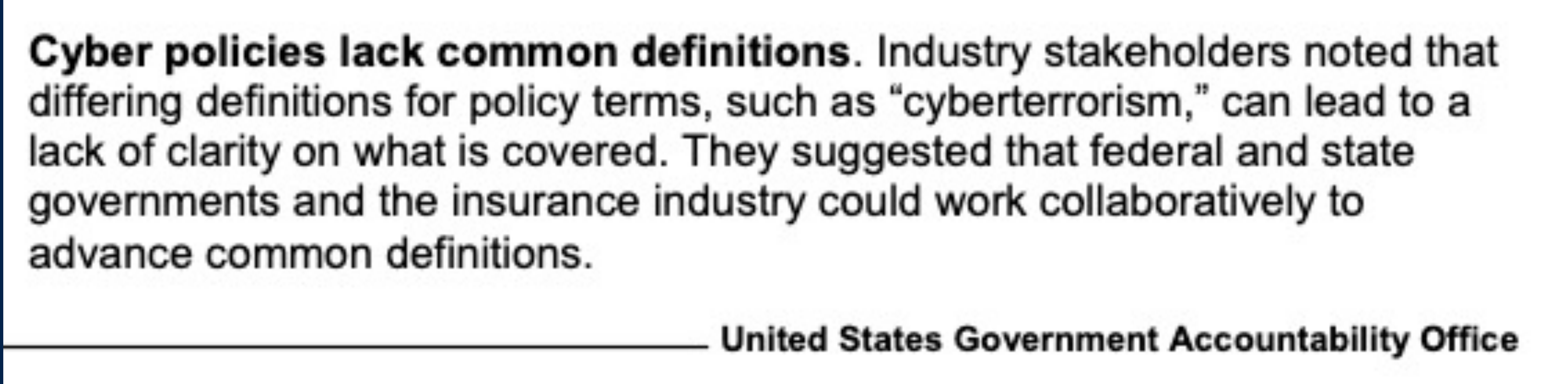
- Avoid
- Accept
- Mitigate
- Transfer



Cyber Insurance is More Important than Ever

- Reduces average cost of a breach by $240,488
- Covers response costs:
  - Incident response specialists
  - Legal services
  - Forensic investigation
  - Threat hunting
  - Public relations
  - Notification costs
  - Etc.
- Business disruption/lost revenue
- Information security/privacy liability
- Regulatory fines (state/federal laws, etc.)

It’s Not Apples to Apples



Cyber policies lack common definitions. Industry stakeholders noted that differing definitions for policy terms, such as "cyberterrorism," can lead to a lack of clarity on what is covered. They suggested that federal and state governments and the insurance industry could work collaboratively to advance common definitions.

United States Government Accountability Office

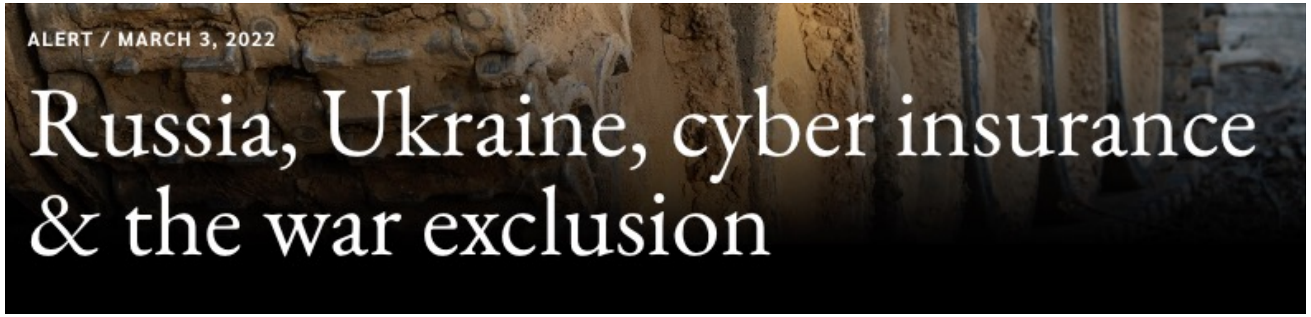
"This ambiguity can result in misunderstandings and litigation between insurers and policyholders." – GAO

https://www.gao.gov/products/gao-21-477

©LMG Security 2021. All rights reserved. | www.LMGsecurity.com

Shifting Cyber Insurance Landscape

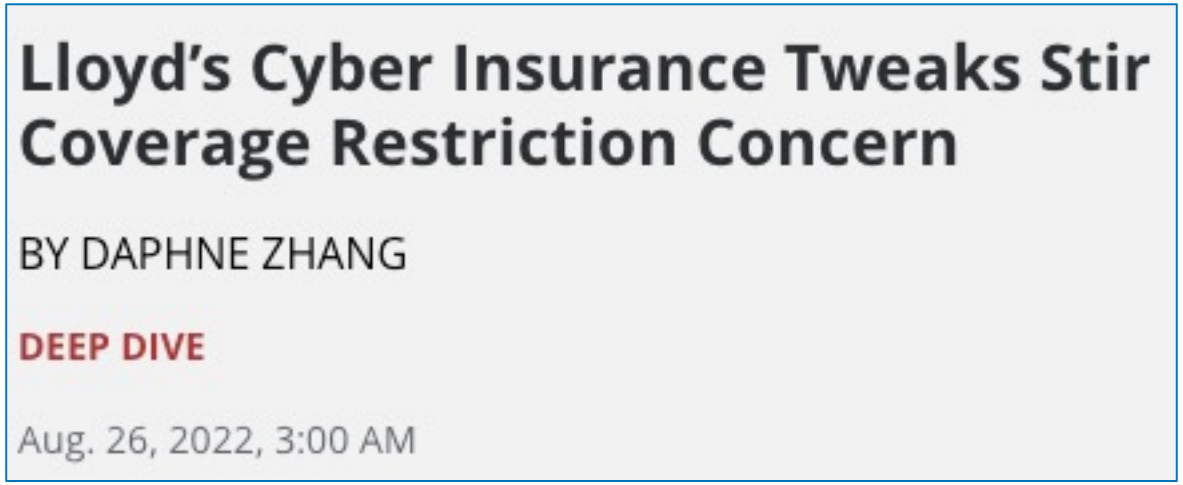
- Acts of War – new requirements from Lloyd's
- Systemic Risks
  - New! Outage of major service providers (Microsoft, Amazon, etc.)
  - Widespread events (ie if a hack affects more than a certain # of organizations, you won't be covered)



ALERT / MARCH 3, 2022

Russia, Ukraine, cyber insurance & the war exclusion

Ensure the cyber insurance coverage is aligned with risks and leadership's risk appetite



Lloyd's Cyber Insurance Tweaks Stir Coverage Restriction Concern

BY DAPHNE ZHANG

DEEP DIVE

Aug. 26, 2022, 3:00 AM

Effective Cybersecurity Starts at the Top

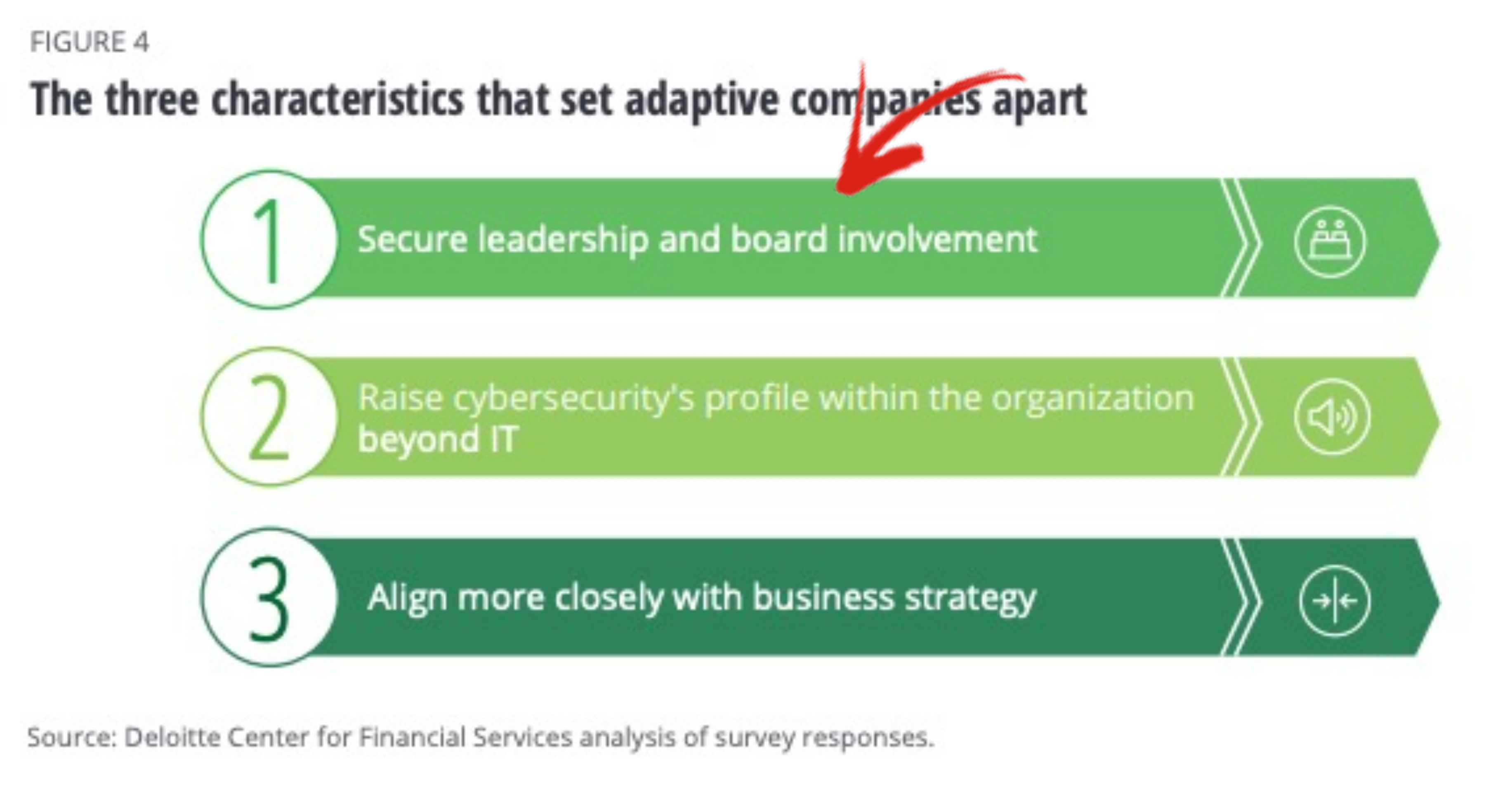


FIGURE 4

The three characteristics that set adaptive companies apart

1 Secure leadership and board involvement

2 Raise cybersecurity's profile within the organization beyond IT

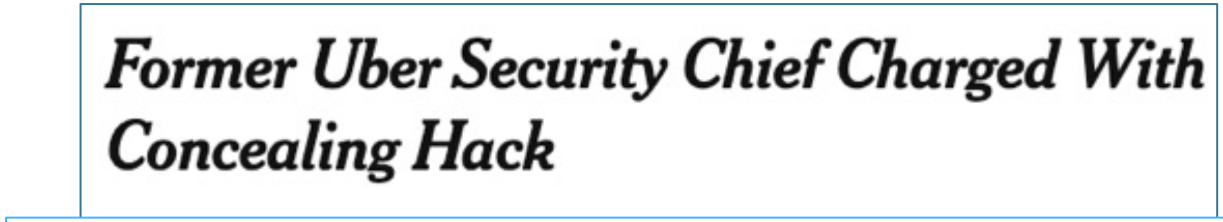
3 Align more closely with business strategy

Source: Deloitte Center for Financial Services analysis of survey responses.

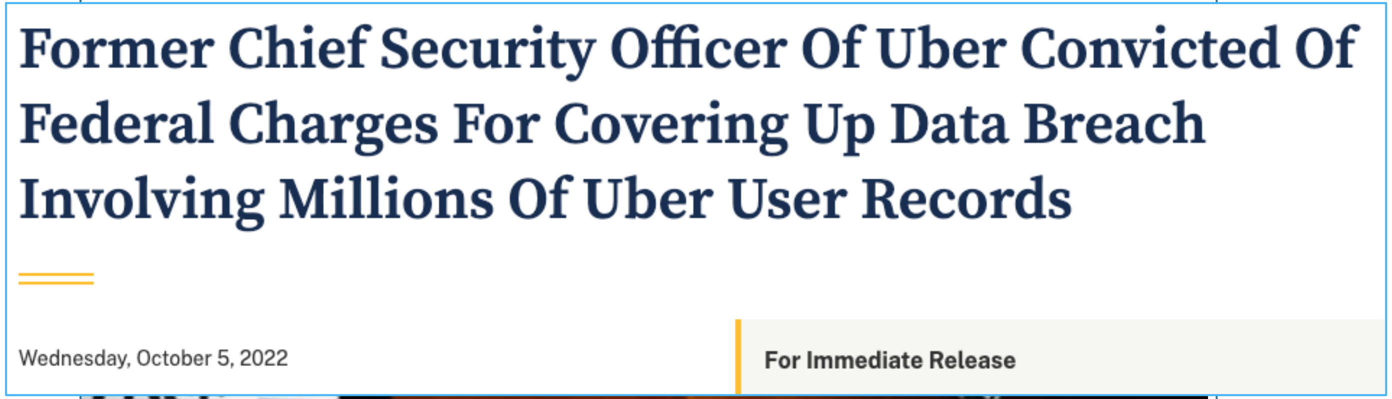
https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/financial-services/DI_Pursuing-cybersecurity-maturity-at-financial-institutions.pdf

©LMG Security 2021. All rights reserved.

Increasing Risks for Management & Board



Former Uber Security Chief Charged With Concealing Hack



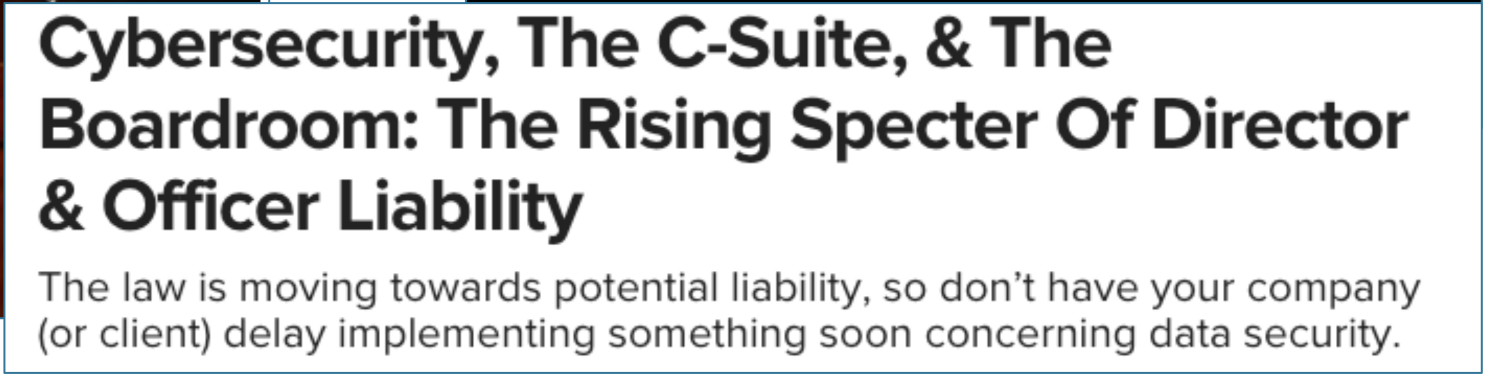
Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records

Wednesday, October 5, 2022

For Immediate Release

Sep 2, 2020

GARTNER WARNS CEOS WILL BE PERSONALLY LIABLE FOR BREACHES BY 2024



Cybersecurity, The C-Suite, & The Boardroom: The Rising Specter Of Director & Officer Liability

The law is moving towards potential liability, so don't have your company (or client) delay implementing something soon concerning data security.

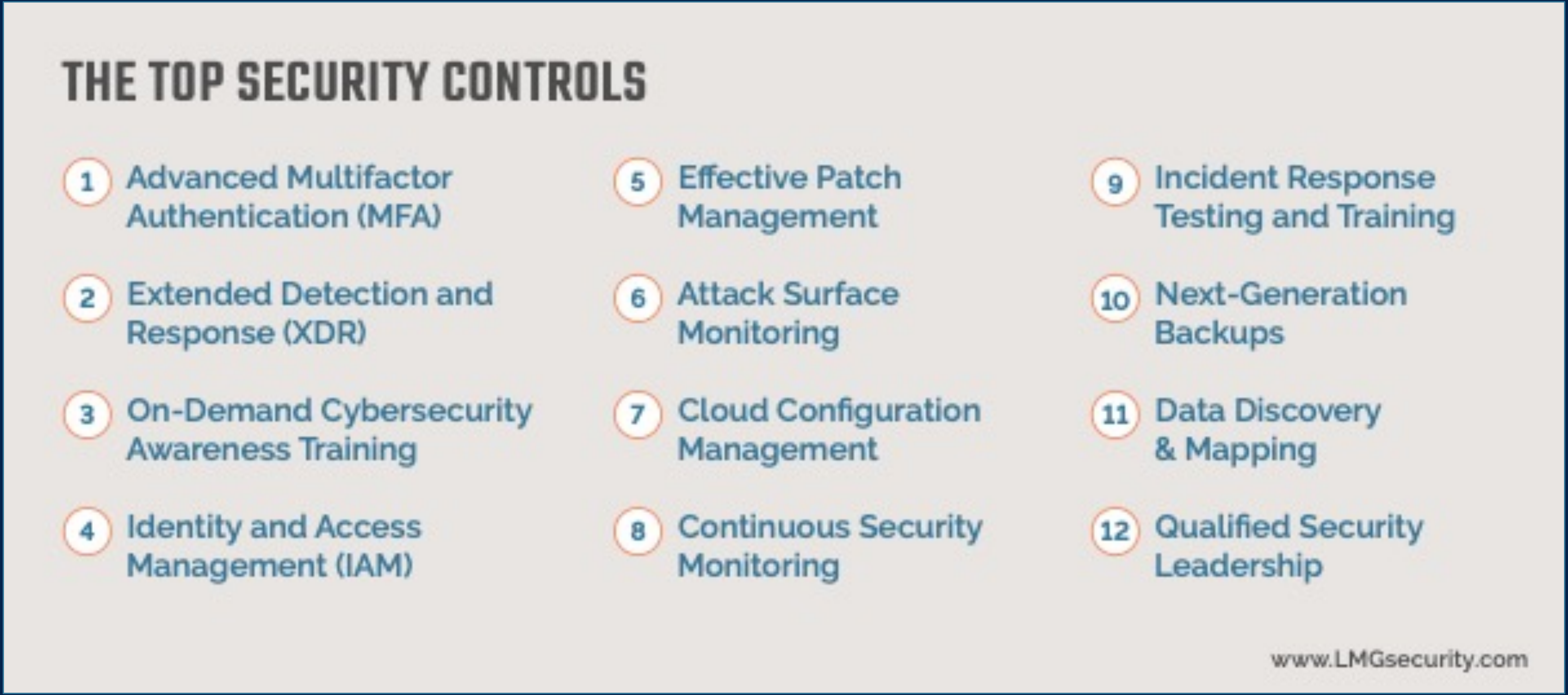
Board & Executive Awareness is Key

- Good job today!
- Empower your executives & board
- Education & training on cybersecurity
- Annual update / budget review
- Metrics & reports
- Cybersecurity risks = business risks

How to Run an Effective Cybersecurity Program

1) **Know What You are Trying to Protect**
   - ✓Inventory of Data & Assets
2) **Understand Your Obligations**
   - ✓Statement of Applicable Laws, Regulations, and Obligations
   - ✓Oversight Responsibilities
3) **Monitor Risk**
   - ✓Risk Assessment Report
   - ✓Cybersecurity Controls Assessment
   - ✓Technical Testing
   - ✓Incident Review
4) **Manage Risk**
   - ✓Top Security Controls of 2023

©LMG Security 2021. All rights reserved.



THE TOP SECURITY CONTROLS

1. Advanced Multifactor Authentication (MFA)
2. Extended Detection and Response (XDR)
3. On-Demand Cybersecurity Awareness Training
4. Identity and Access Management (IAM)
5. Effective Patch Management
6. Attack Surface Monitoring
7. Cloud Configuration Management
8. Continuous Security Monitoring
9. Incident Response Testing and Training
10. Next-Generation Backups
11. Data Discovery & Mapping
12. Qualified Security Leadership

www.LMGsecurity.com

https://www.LMGsecurity.com/resources/top-cybersecurity-controls/

Questions?

- Sherri Davidoff, CEO of LMG Security
- info@LMGsecurity.com

@LMGSecurity

sherridavidoff@infosec.exchange

- Find me on LinkedIn

PCBS

The National Graduate School of Banking™

Register now for the Ransomware Response class!
https://www.LMGsecurity.com/ransomwareclass
$50 Discount code for PCBS community: PCBS438

©LMG Security 2021. All rights reserved.