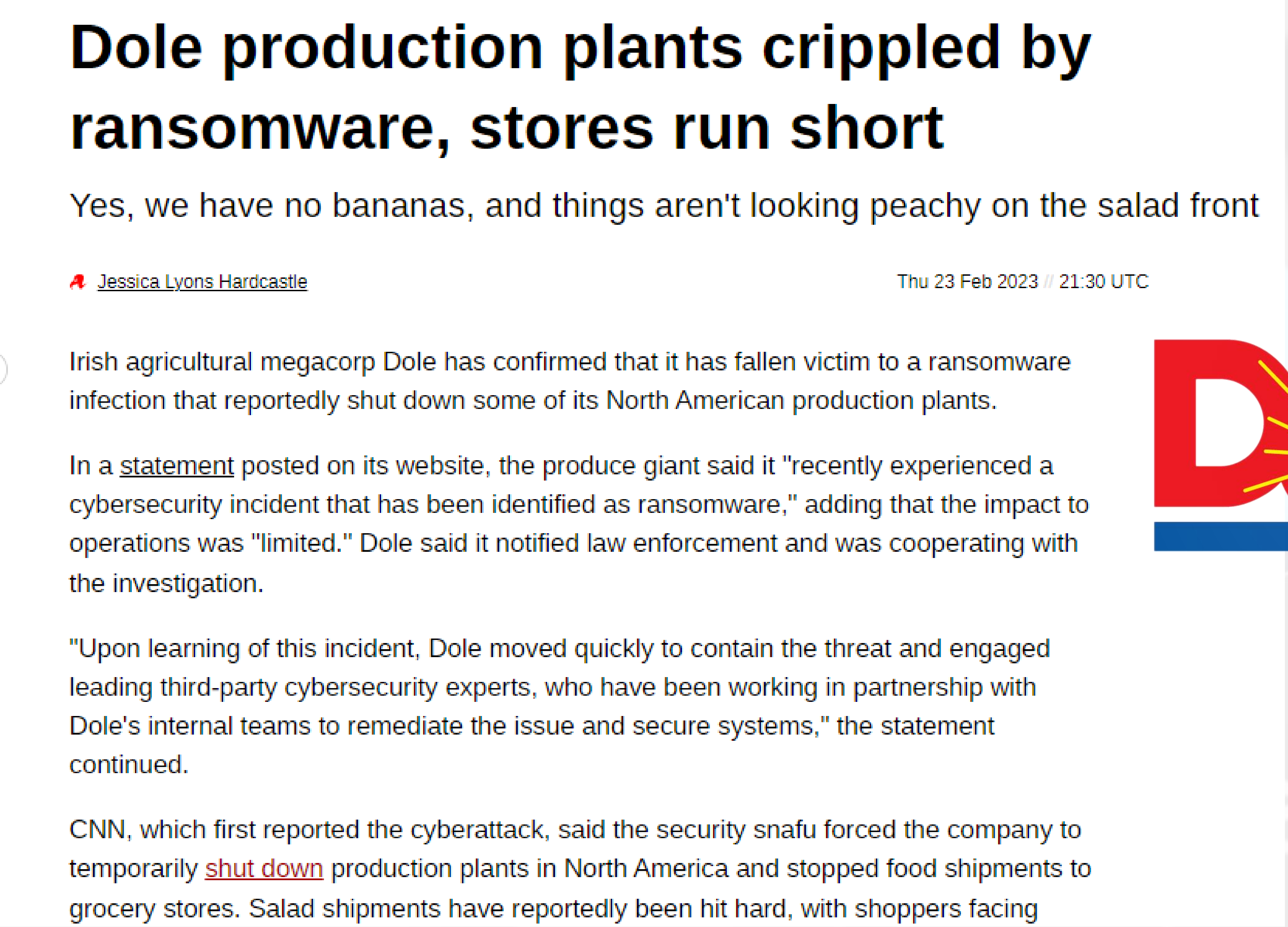
NATIONAL CYBERSECURITY ALLIANCE

ZETA SKY
ELEVATING BUSINESS TECHNOLOGY

Business of Cybercrime

Building your Security Culture



Dole production plants crippled by ransomware, stores run short

Yes, we have no bananas, and things aren't looking peachy on the salad front

Jessica Lyons Hardcastle

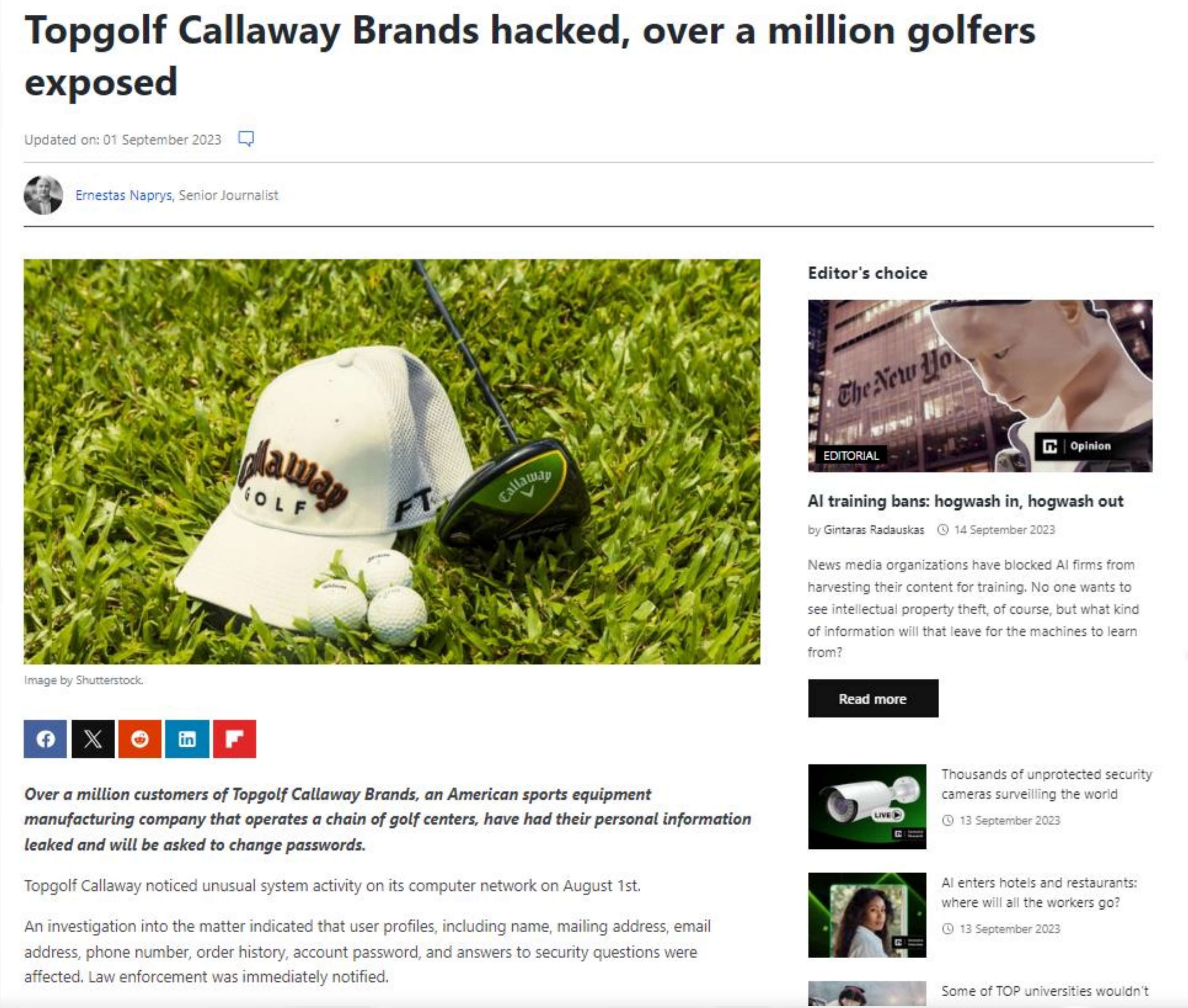
Thu 23 Feb 2023 // 21:30 UTC

Irish agricultural megacorp Dole has confirmed that it has fallen victim to a ransomware infection that reportedly shut down some of its North American production plants.

In a statement posted on its website, the produce giant said it "recently experienced a cybersecurity incident that has been identified as ransomware," adding that the impact to operations was "limited." Dole said it notified law enforcement and was cooperating with the investigation.

"Upon learning of this incident, Dole moved quickly to contain the threat and engaged leading third-party cybersecurity experts, who have been working in partnership with Dole's internal teams to remediate the issue and secure systems," the statement continued.

CNN, which first reported the cyberattack, said the security snafu forced the company to temporarily shut down production plants in North America and stopped food shipments to grocery stores. Salad shipments have reportedly been hit hard, with shoppers facing



Topgolf Callaway Brands hacked, over a million golfers exposed

Updated on: 01 September 2023

Ernestas Naprys, Senior Journalist

Image by Shutterstock.

Over a million customers of Topgolf Callaway Brands, an American sports equipment manufacturing company that operates a chain of golf centers, have had their personal information leaked and will be asked to change passwords.

Topgolf Callaway noticed unusual system activity on its computer network on August 1st.

An investigation into the matter indicated that user profiles, including name, mailing address, email address, phone number, order history, account password, and answers to security questions were affected. Law enforcement was immediately notified.

Editor's choice

AI training bans: hogwash in, hogwash out

by Gintaras Radauskas 14 September 2023

News media organizations have blocked AI firms from harvesting their content for training. No one wants to see intellectual property theft, of course, but what kind of information will that leave for the machines to learn from?

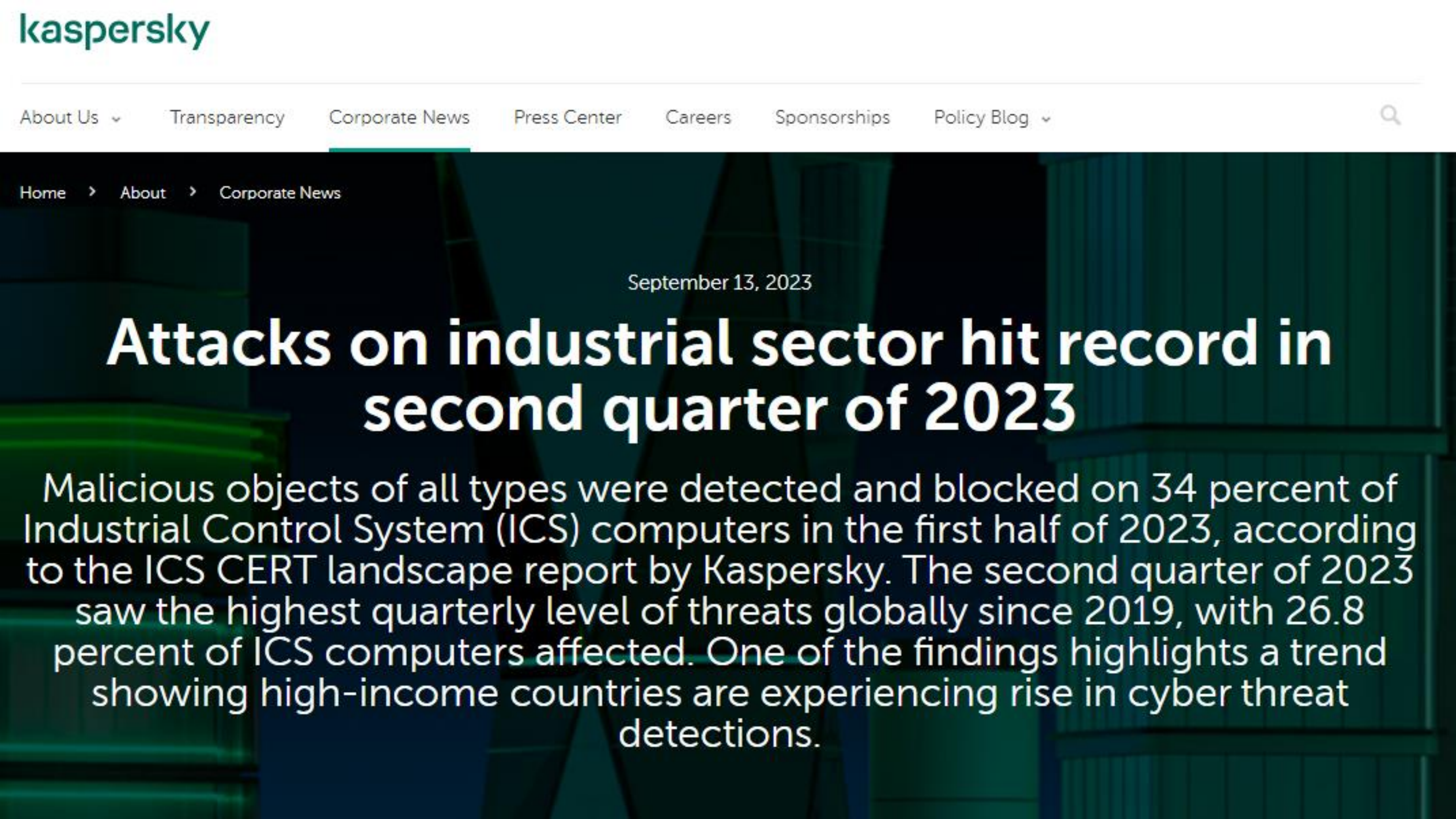
Thousands of unprotected security cameras surveilling the world

13 September 2023

AI enters hotels and restaurants: where will all the workers go?

13 September 2023

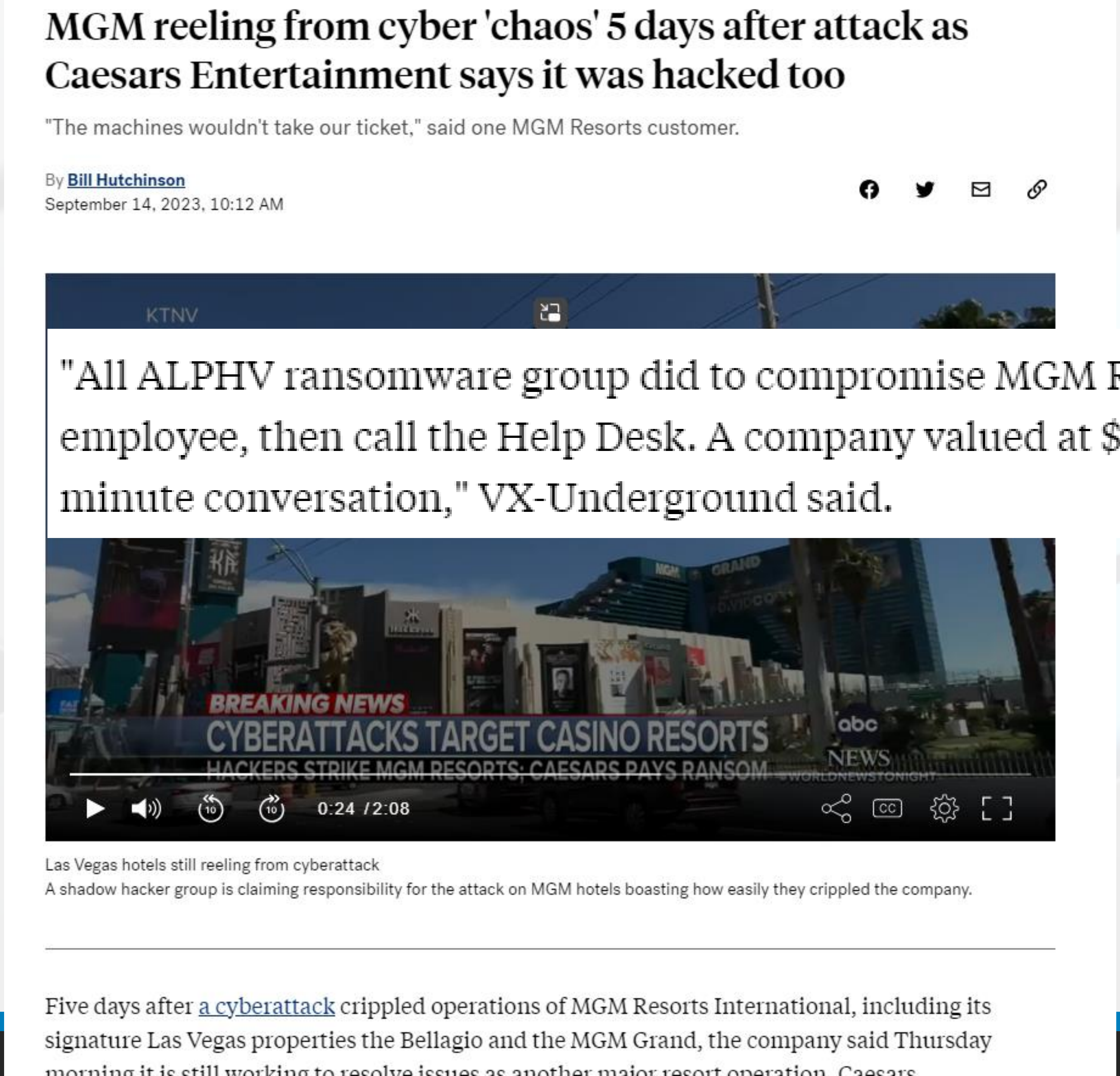
Some of TOP universities wouldn't



September 13, 2023

Attacks on industrial sector hit record in second quarter of 2023

Malicious objects of all types were detected and blocked on 34 percent of Industrial Control System (ICS) computers in the first half of 2023, according to the ICS CERT landscape report by Kaspersky. The second quarter of 2023 saw the highest quarterly level of threats globally since 2019, with 26.8 percent of ICS computers affected. One of the findings highlights a trend showing high-income countries are experiencing rise in cyber threat detections.



MGM reeling from cyber 'chaos' 5 days after attack as Caesars Entertainment says it was hacked too

"The machines wouldn't take our ticket," said one MGM Resorts customer.

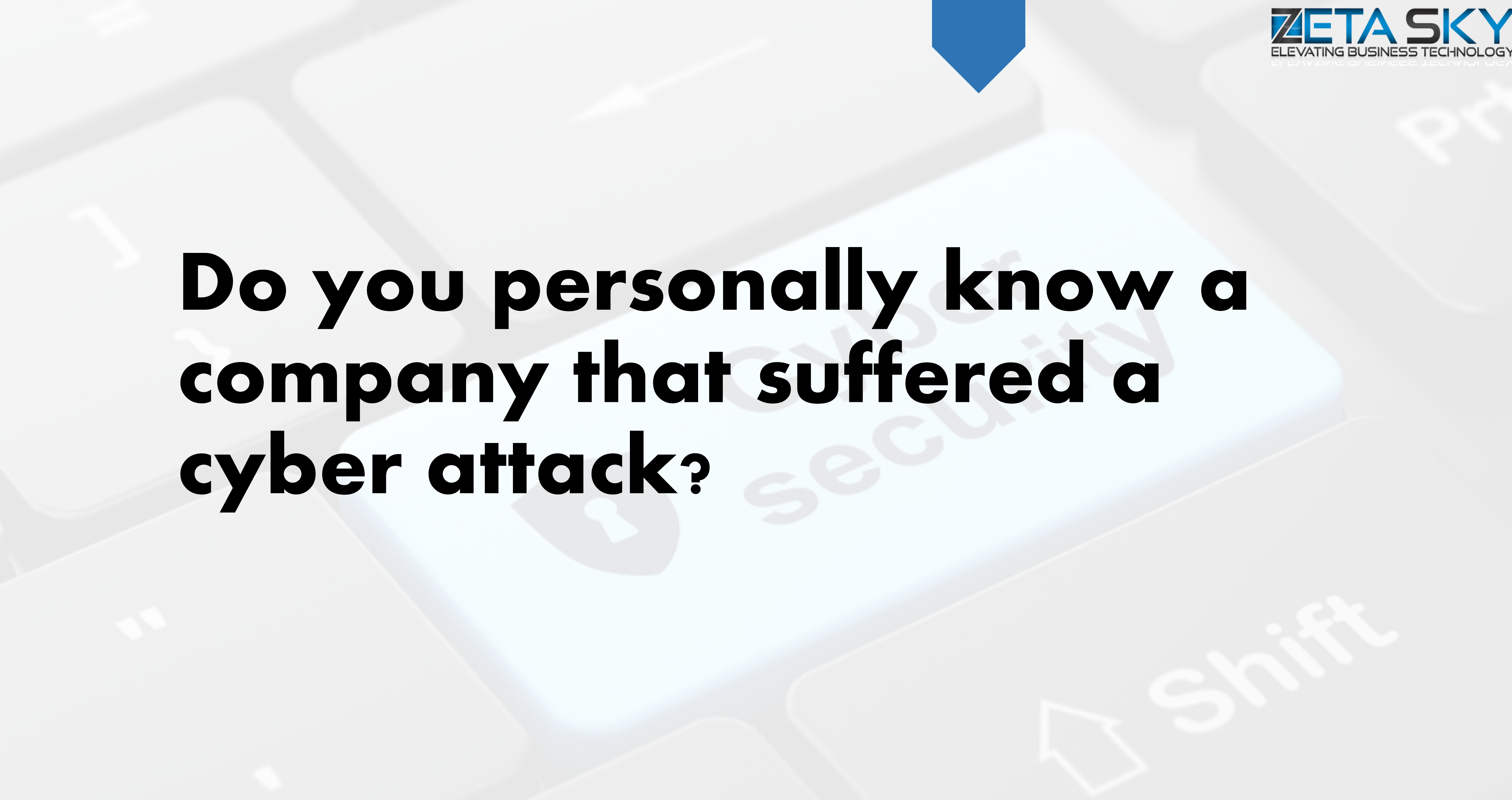
By Bill Hutchinson
September 14, 2023, 10:12 AM

KTNV
BREAKING NEWS
CYBERATTACKS TARGET CASINO RESORTS
HACKERS STRIKE MGM RESORTS; CAESARS PAYS RANSOM
abc NEWS
#WORLDNEWSTONIGHT
0:24 /2:08

"All ALPHV ransomware group did to compromise MGM Resorts was hop on LinkedIn, find an employee, then call the Help Desk. A company valued at $33,900,000,000 was defeated by a 10-minute conversation," VX-Underground said.

Las Vegas hotels still reeling from cyberattack
A shadow hacker group is claiming responsibility for the attack on MGM hotels boasting how easily they crippled the company.

Five days after a cyberattack crippled operations of MGM Resorts International, including its signature Las Vegas properties the Bellagio and the MGM Grand, the company said Thursday morning it is still working to resolve issues as another major resort operation, Caesars



Do you personally know a company that suffered a cyber attack?

Can you find the story in the news?

Who Am I?...

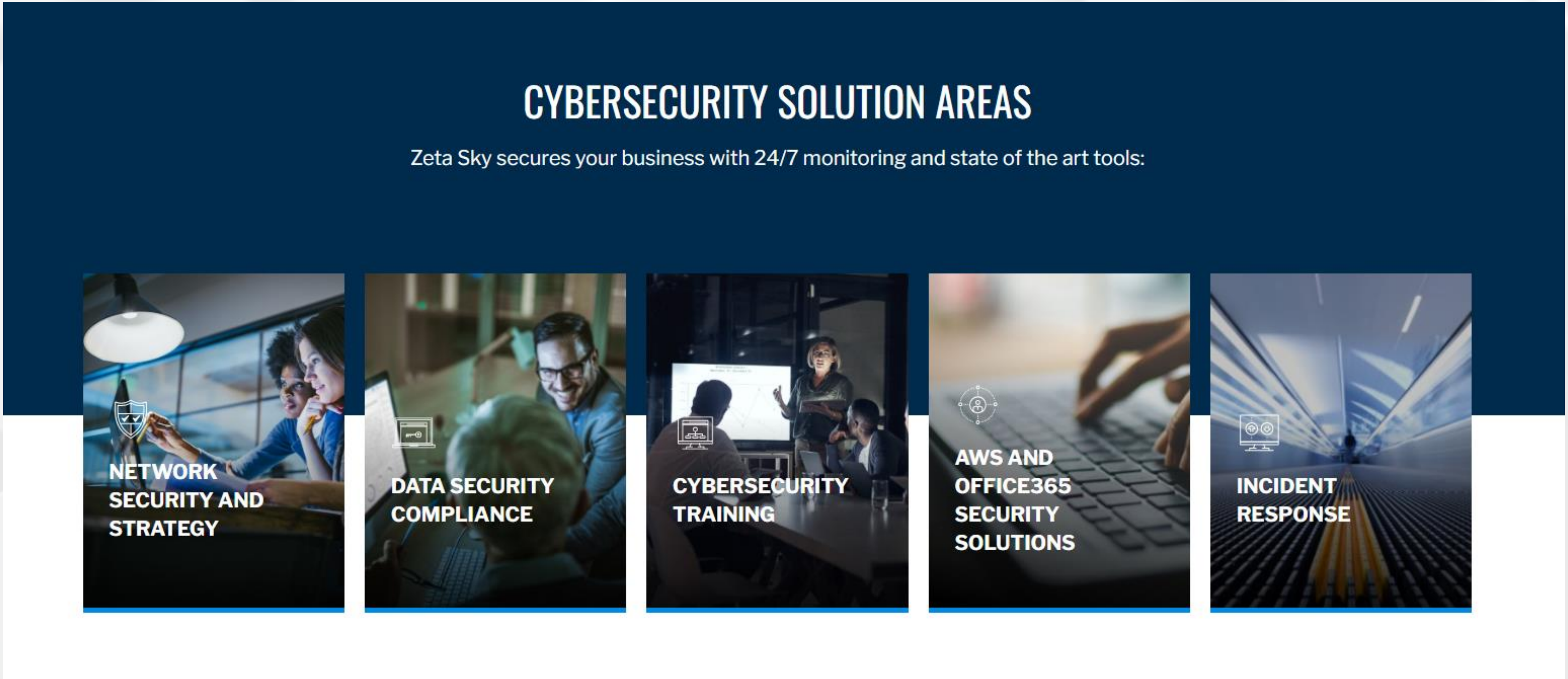
Adrian Francoz

- **CEO & Co-Founder of Zeta Sky**
  - Manage cybersecurity defense for companies ranging from small businesses to small enterprises.
  - Work with corporate leaders and IT teams to build their cybersecurity culture and implement a multi-layered defense system.
- **Our team manages cybersecurity for over 100 organizations nationwide**
- **Educate business leaders on how to protect their company and employees**

Involved at the forefront...

NATIONAL
CYBERSECURITY
ALLIANCE

ORANGE COUNTY
SMALL BUSINESS
TECH DAY



CYBERSECURITY SOLUTION AREAS

Zeta Sky secures your business with 24/7 monitoring and state of the art tools:

NETWORK SECURITY AND STRATEGY

DATA SECURITY COMPLIANCE

CYBERSECURITY TRAINING

AWS AND OFFICE365 SECURITY SOLUTIONS

INCIDENT RESPONSE

Business of Cyber-crime

$Multi-Billion Annual Market- Growing

- 5.3 Billion Internet Users 2023
  - Compared to 2 Billion in 2015
  - Over $2 trillion in losses globally (Juniper Research)
  - avg. cost of cyber-attack is $4.45 million (IBM)

Personal, Small, Medium,& Large Corporations

- Myth that hackers are only interested in big companies

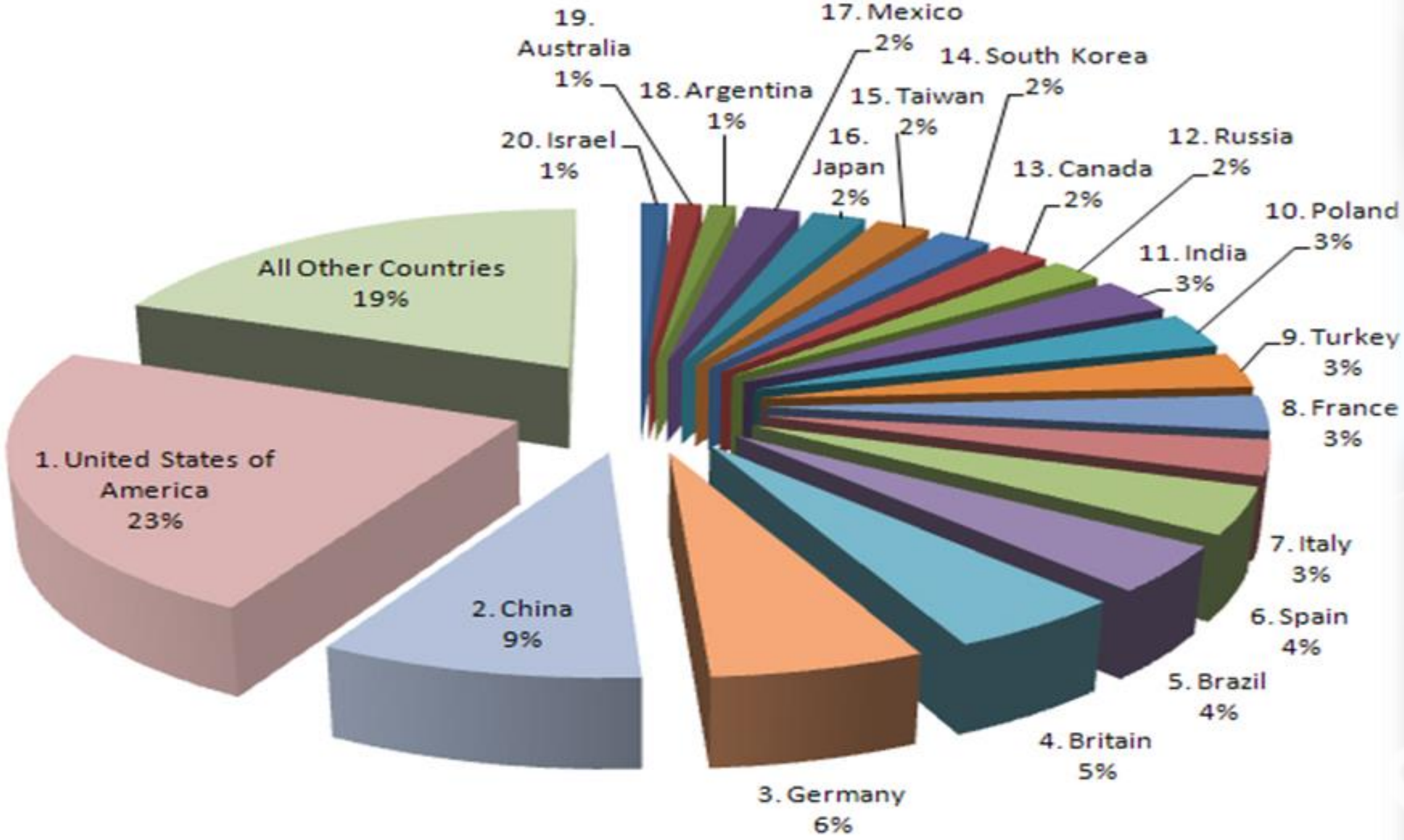
Mostly Reactive Industry

- Hackers create a vulnerability and succeed
- Defense companies react and block

What Does a Cyber Criminal Look Like?

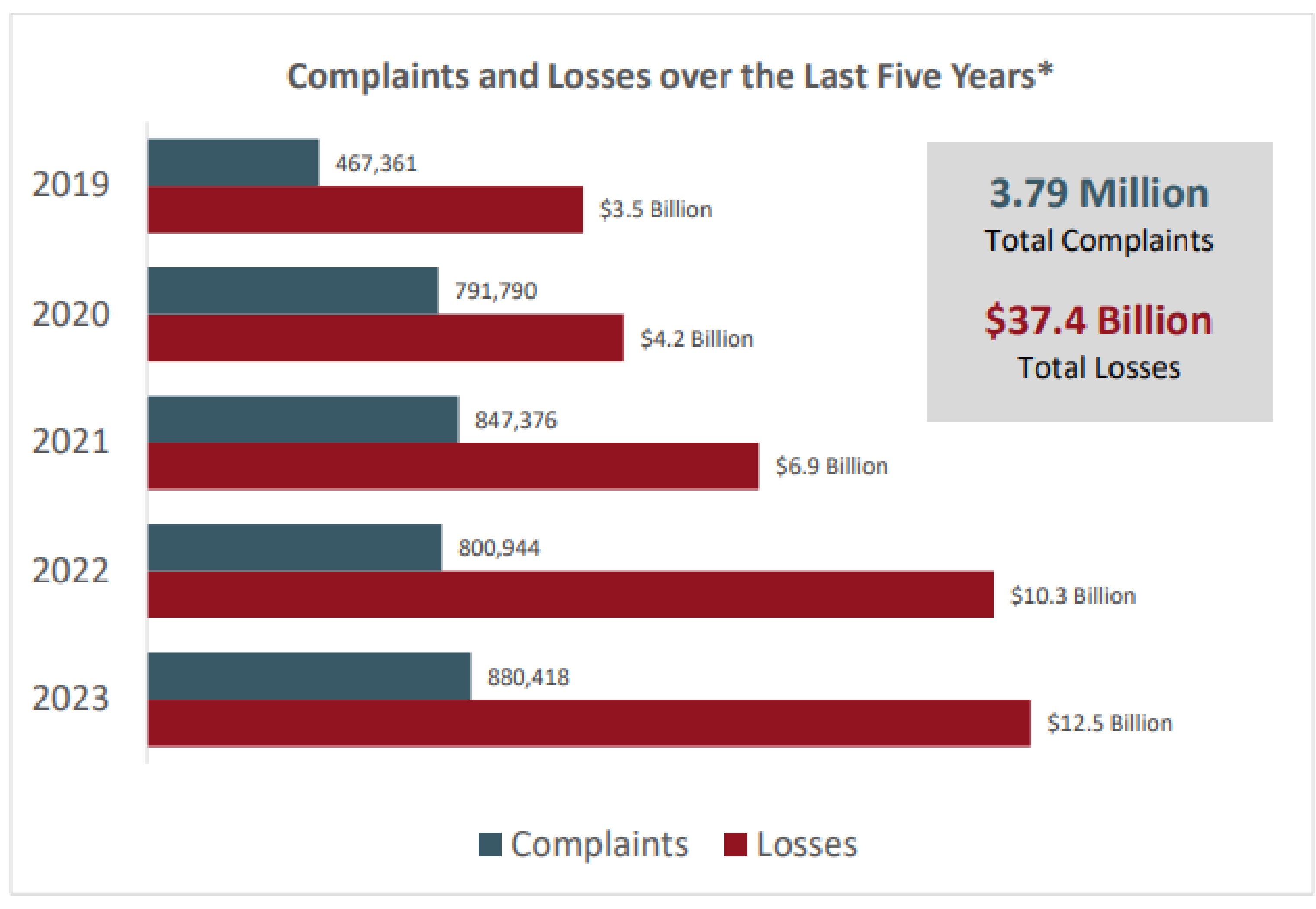
NO SMO... PLEASE
IT'S FUN TO USE LEARNING FOR EVIL!
ACTUAL SIZE!

Business of Cyber-crime

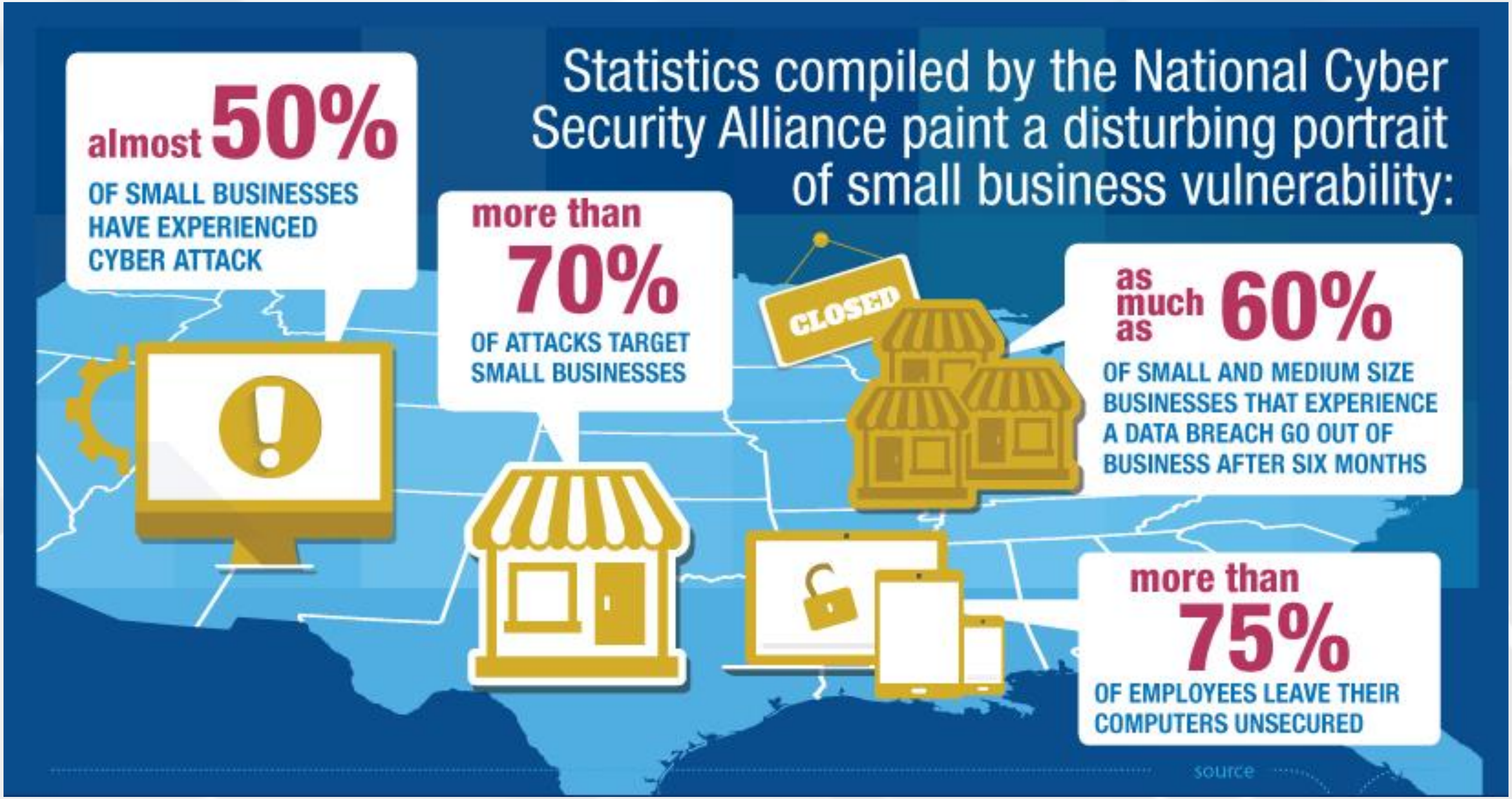


Cybercrime: Top 20 Countries

FBI IC3 Report


Complaints and Losses over the Last Five Years*

Business of Cyber-crime



Statistics compiled by the National Cyber Security Alliance paint a disturbing portrait of small business vulnerability:

almost **50%** OF SMALL BUSINESSES HAVE EXPERIENCED CYBER ATTACK

more than **70%** OF ATTACKS TARGET SMALL BUSINESSES

as much as **60%** OF SMALL AND MEDIUM SIZE BUSINESSES THAT EXPERIENCE A DATA BREACH GO OUT OF BUSINESS AFTER SIX MONTHS

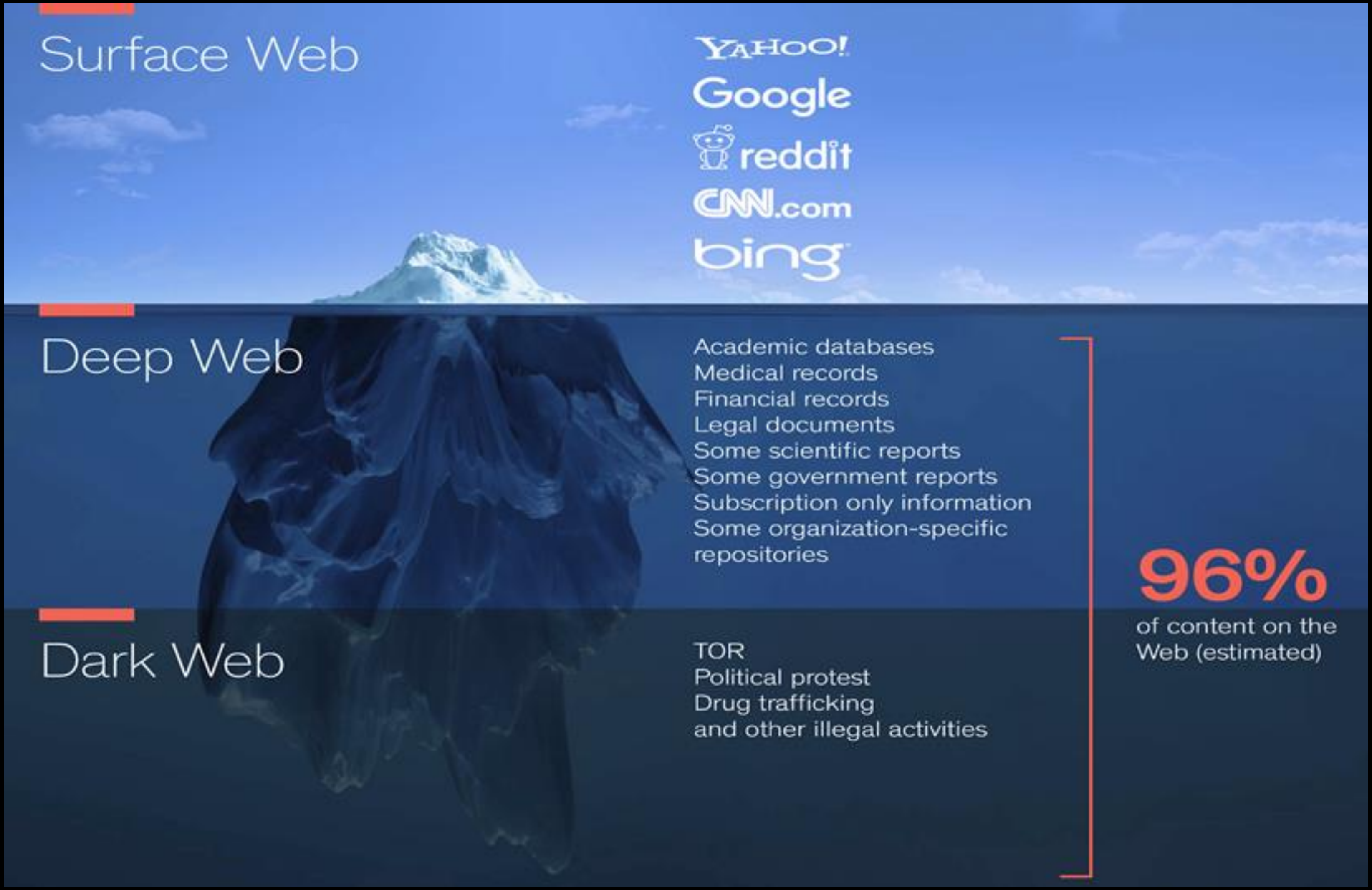
more than **75%** OF EMPLOYEES LEAVE THEIR COMPUTERS UNSECURED

source

Threat Groups

- Ransomware Developers
- Insider Threats
- Organized Crime
- Nation State
- IoT Hackers

Anatomy of the Internet



Surface Web

YAHOO!
Google
reddit
CNN.com
bing

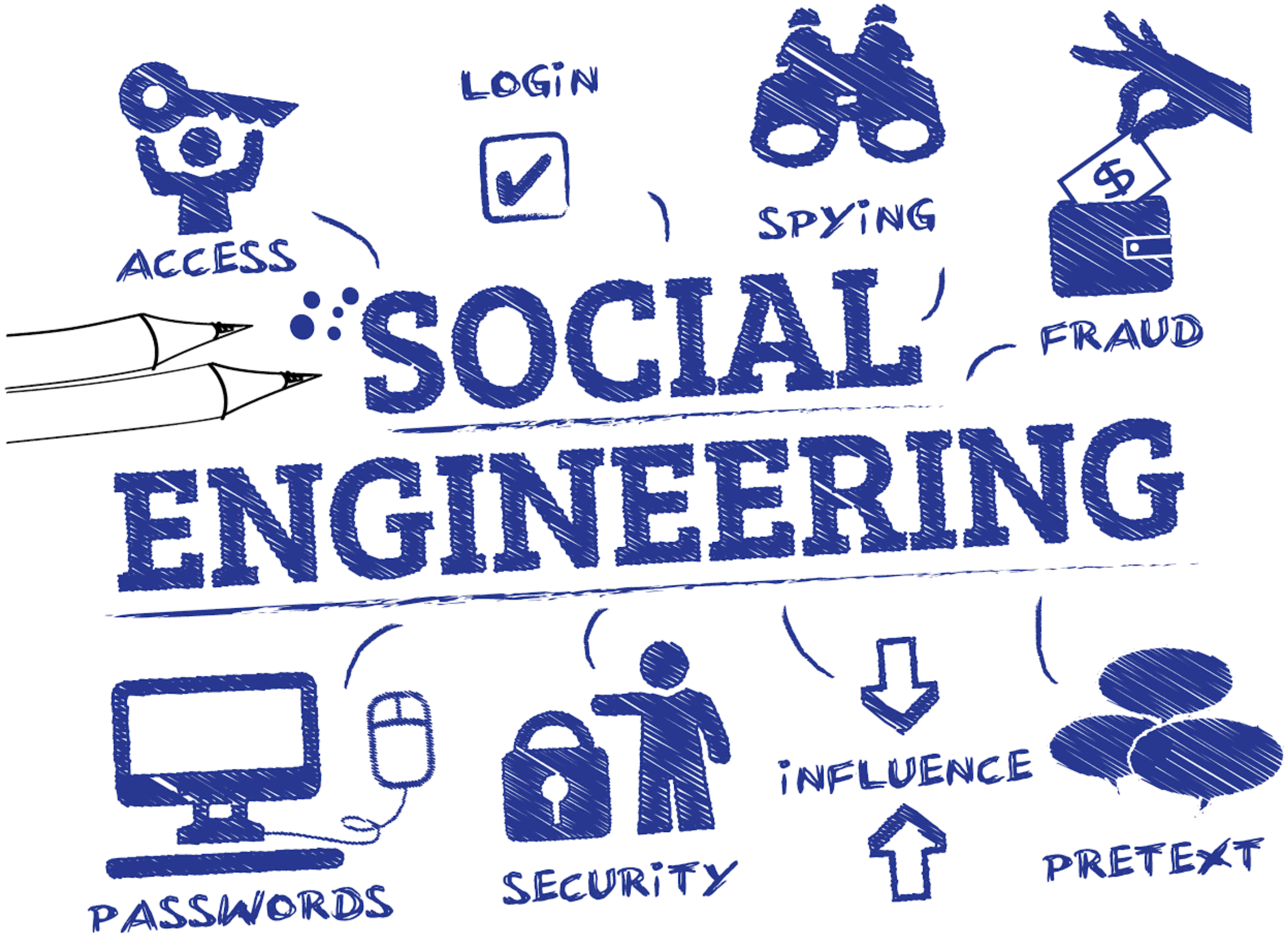
Deep Web

Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription only information
Some organization-specific repositories

Dark Web

TOR
Political protest
Drug trafficking
and other illegal activities

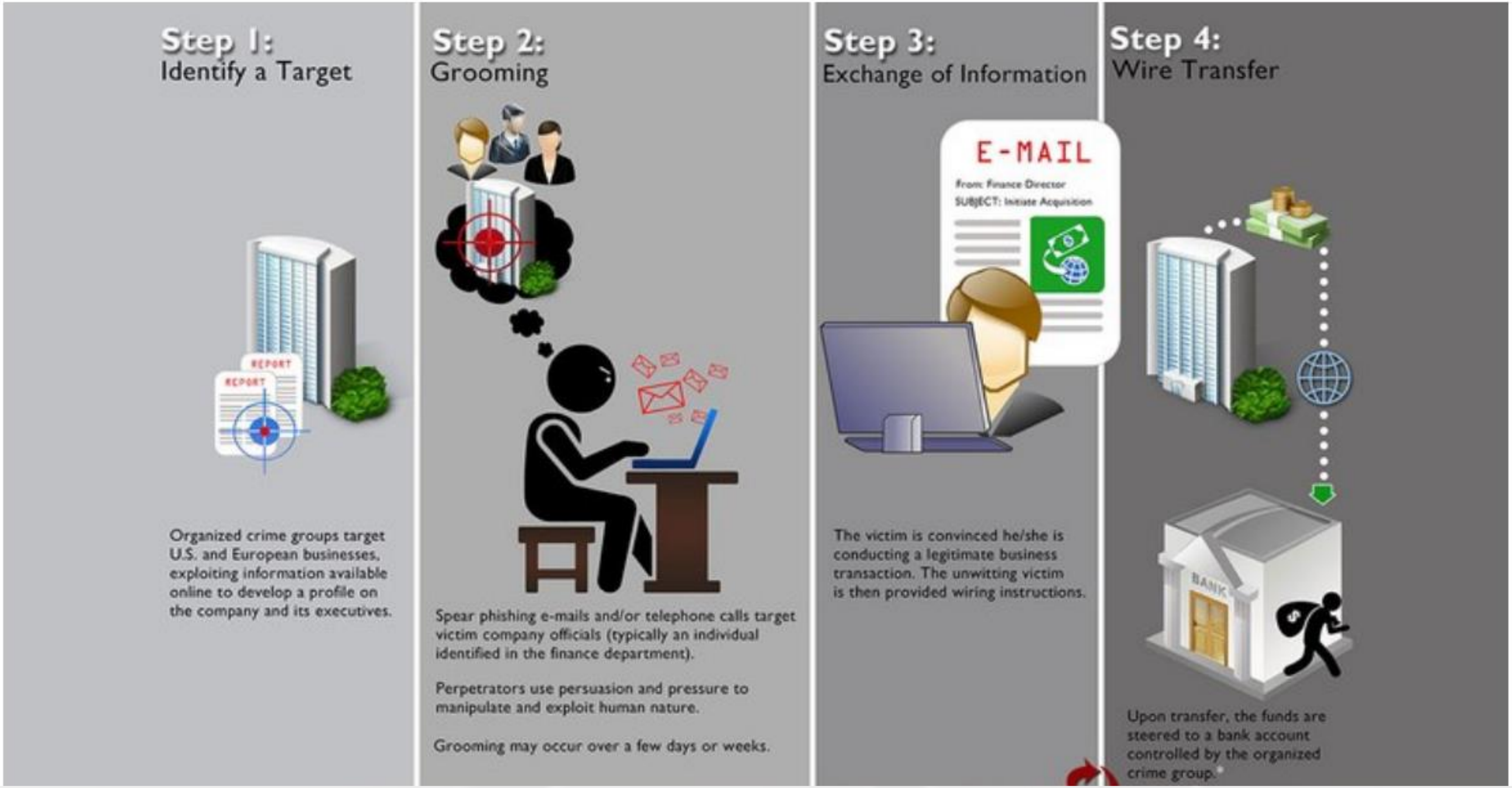
96%
of content on the Web (estimated)


ACCESS
LOGIN
SPYING
FRAUD
SOCIAL
ENGINEERING
PASSWORDS
SECURITY
INFLUENCE
PRETEXT

LOGIN
PASSWORD

Business E-Mail Compromise

Cyber-Enabled Financial Fraud on the Rise Globally



Step 1:
Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2:
Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3:
Exchange of Information

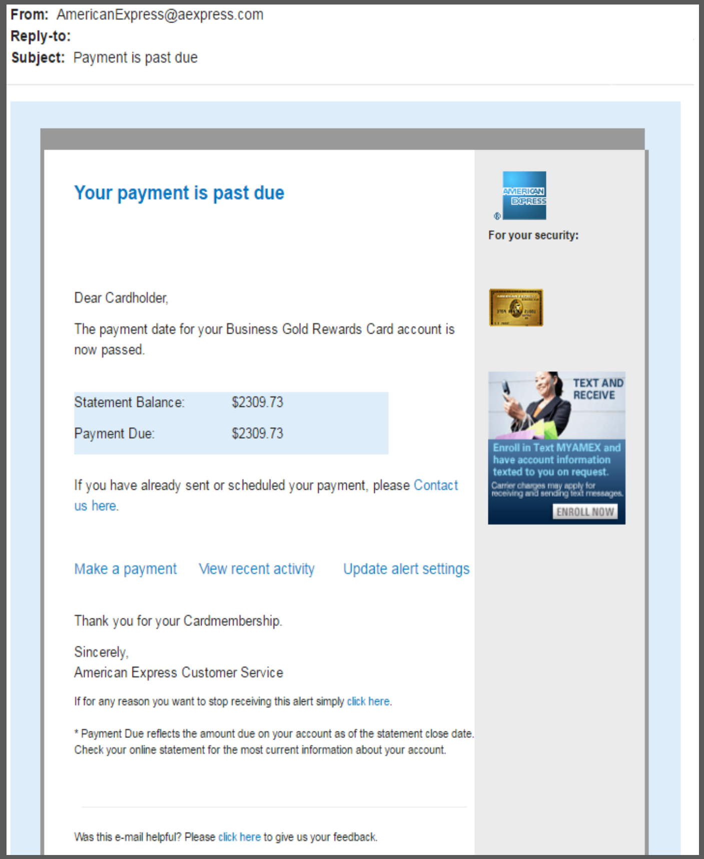
E-MAIL
From: Finance Director
SUBJECT: Initiate Acquisition

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4:
Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.

Common Phishing Emails



From: AmericanExpress@aexpress.com
Reply-to:
Subject: Payment is past due

Your payment is past due

Dear Cardholder,

The payment date for your Business Gold Rewards Card account is now passed.

Statement Balance:	$2309.73
Payment Due:	$2309.73

If you have already sent or scheduled your payment, please Contact us here.

Make a payment   View recent activity   Update alert settings

Thank you for your Cardmembership.

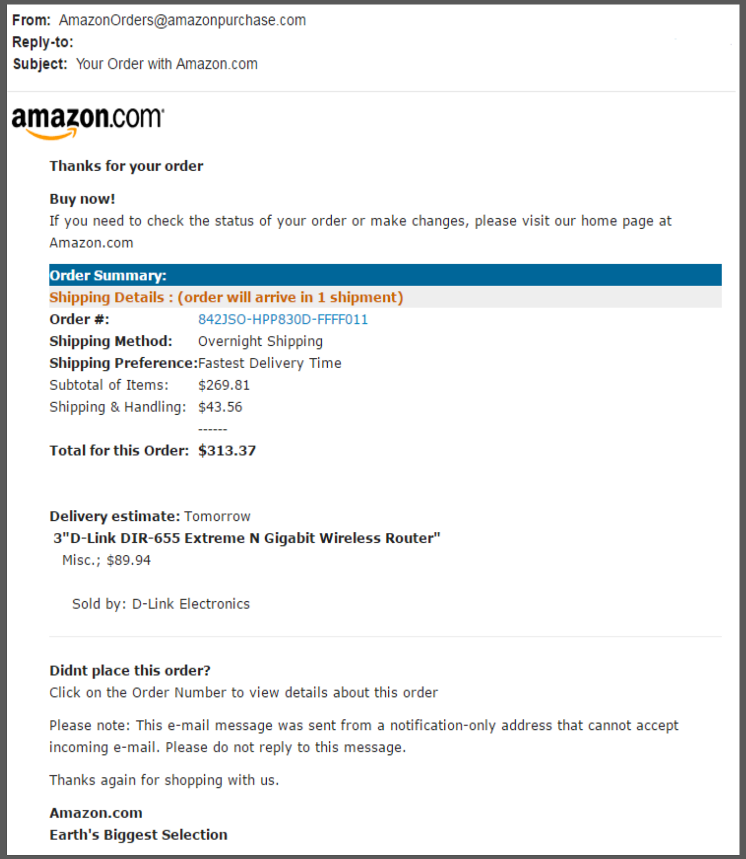
Sincerely,
American Express Customer Service

If for any reason you want to stop receiving this alert simply click here.

* Payment Due reflects the amount due on your account as of the statement close date. Check your online statement for the most current information about your account.

Was this e-mail helpful? Please click here to give us your feedback.

TEXT AND RECEIVE
Enroll in Text MYAMEX and have account information texted to you on request.
Carrier charges may apply for receiving and sending text messages.
ENROLL NOW



From: AmazonOrders@amazonpurchase.com
Reply-to:
Subject: Your Order with Amazon.com

amazon.com

Thanks for your order

Buy now!
If you need to check the status of your order or make changes, please visit our home page at Amazon.com

Order Summary:
Shipping Details : (order will arrive in 1 shipment)

Order #:	842JSO-HPP830D-FFFF011
Shipping Method:	Overnight Shipping
Shipping Preference:	Fastest Delivery Time
Subtotal of Items:	$269.81
Shipping & Handling:	$43.56

Total for this Order:	**$313.37**

Delivery estimate: Tomorrow
3"D-Link DIR-655 Extreme N Gigabit Wireless Router"
Misc.; $89.94

Sold by: D-Link Electronics

Didnt place this order?
Click on the Order Number to view details about this order

Please note: This e-mail message was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Thanks again for shopping with us.

Amazon.com
Earth's Biggest Selection

Network Vulnerabilities Footprint Growing

Artificial Intelligence

- **Deep Fake Audio / Video Generation**
  - Voice Cloning Scams
  - Phone number scamming
- **Automated Phishing**
  - Chat GPT to write convincing emails with your industry jargon.
- **Hyper-Personalization to make scam convincing.**
- **Bot calls to scale up scams**
- **Developing their own AI apps and selling on Dark Web**

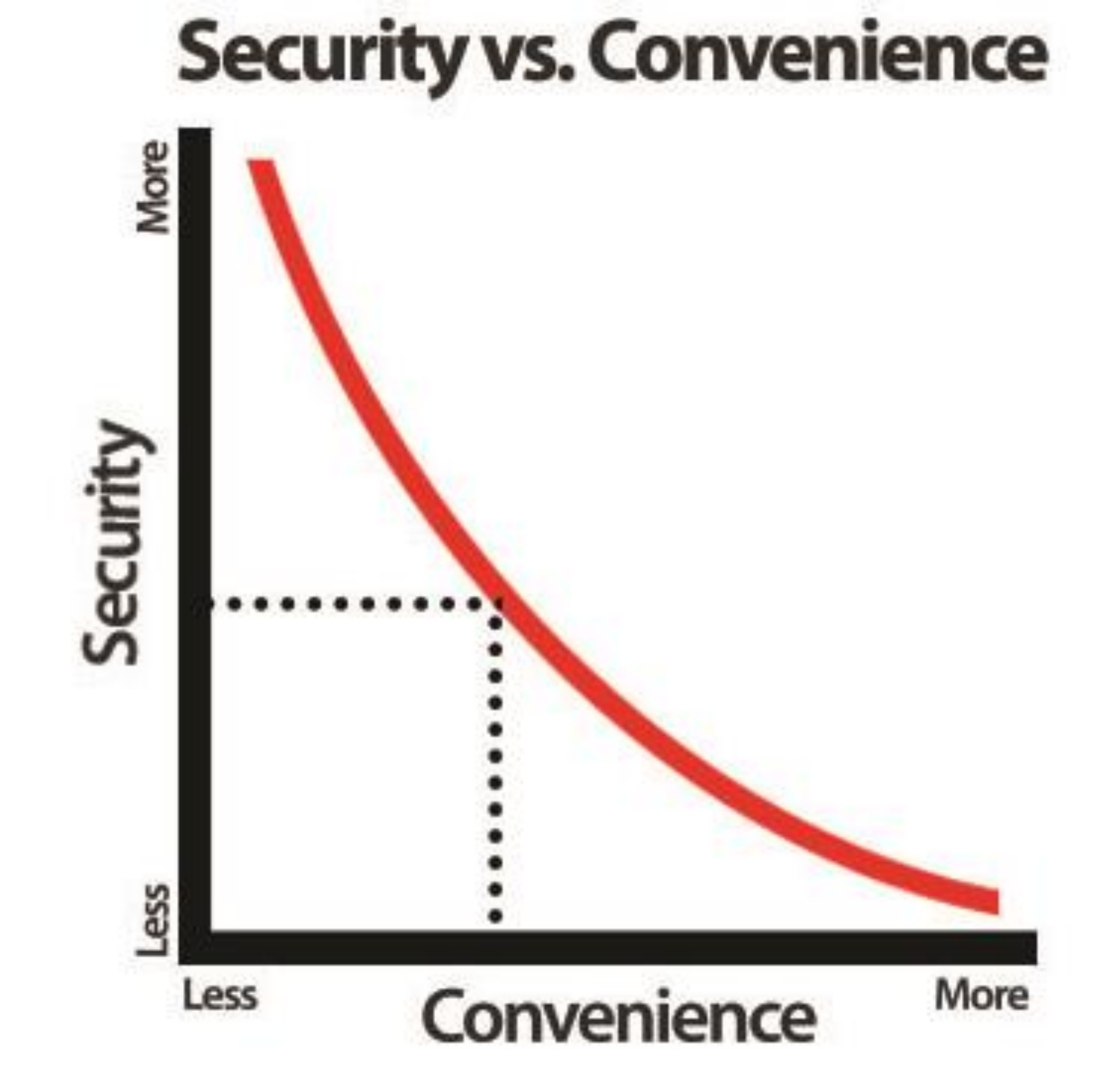
AI HACKERS

How Do You Protect Your Business?

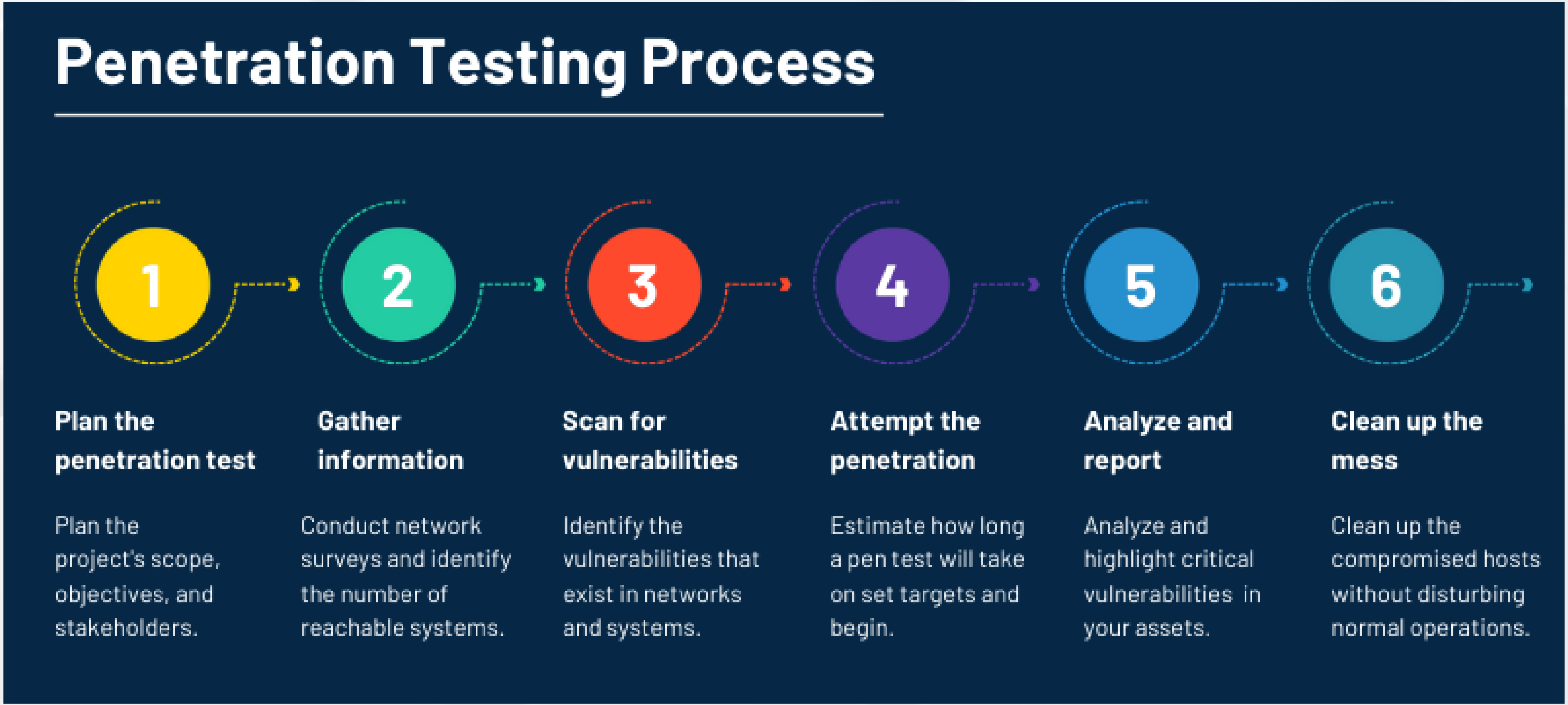
IT ALL STARTS WITH

YOU!

Figuring out your "security culture"



Where are your current vulnerabilities?



Penetration Testing Process

1 **Plan the penetration test**

Plan the project's scope, objectives, and stakeholders.

2 **Gather information**

Conduct network surveys and identify the number of reachable systems.

3 **Scan for vulnerabilities**

Identify the vulnerabilities that exist in networks and systems.

4 **Attempt the penetration**

Estimate how long a pen test will take on set targets and begin.

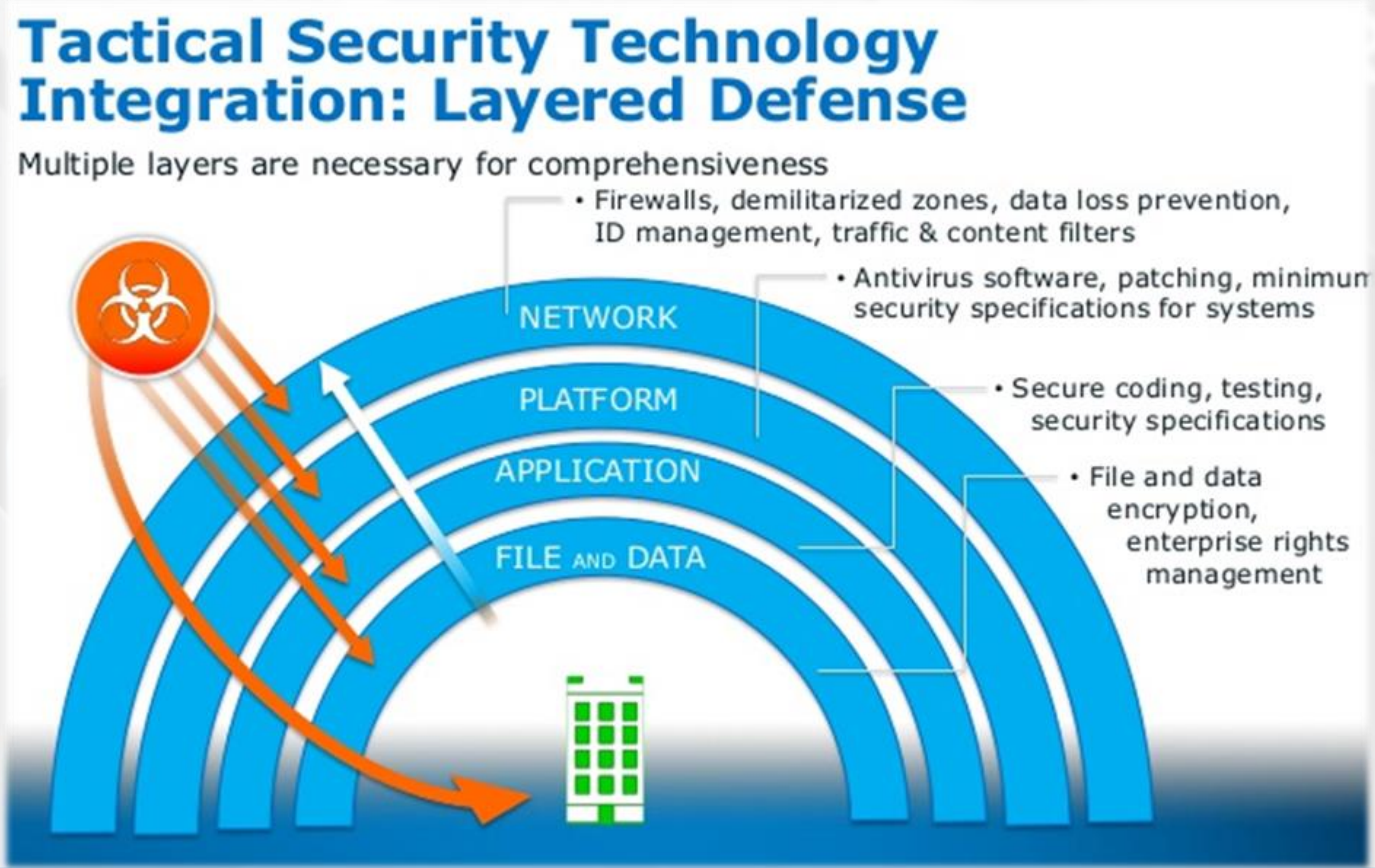
5 **Analyze and report**

Analyze and highlight critical vulnerabilities in your assets.

6 **Clean up the mess**

Clean up the compromised hosts without disturbing normal operations.

Security Layering



Tactical Security Technology Integration: Layered Defense

Multiple layers are necessary for comprehensiveness

- Firewalls, demilitarized zones, data loss prevention, ID management, traffic & content filters
- Antivirus software, patching, minimum security specifications for systems
- Secure coding, testing, security specifications
- File and data encryption, enterprise rights management

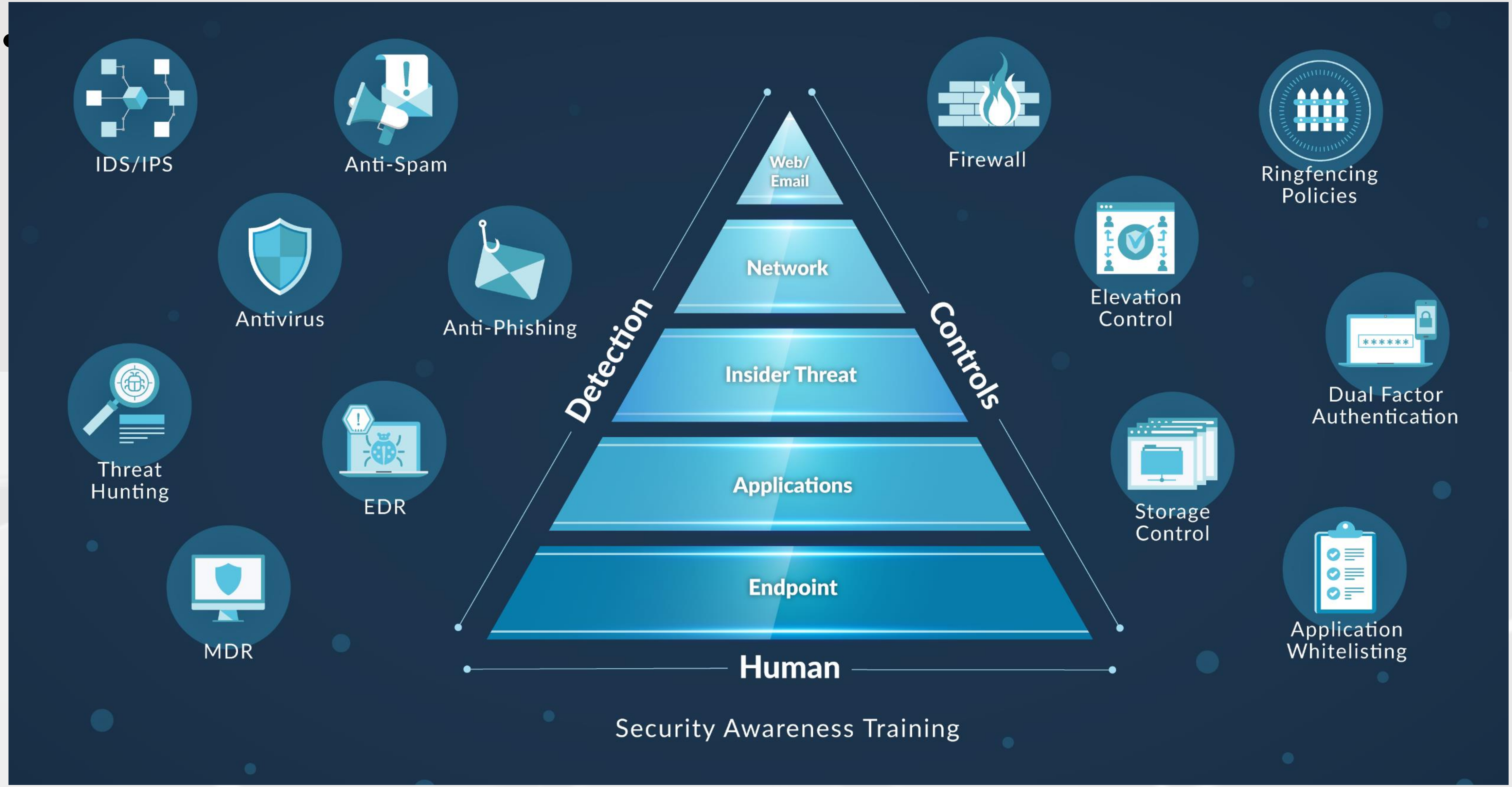
NETWORK

PLATFORM

APPLICATION

FILE AND DATA

Multi Layered Security Approach



The Forgotten Layer…

You… The Human Firewall

We are sinking!! We are sinking!!

Can’t avoid something if you don’t know what it looks like…

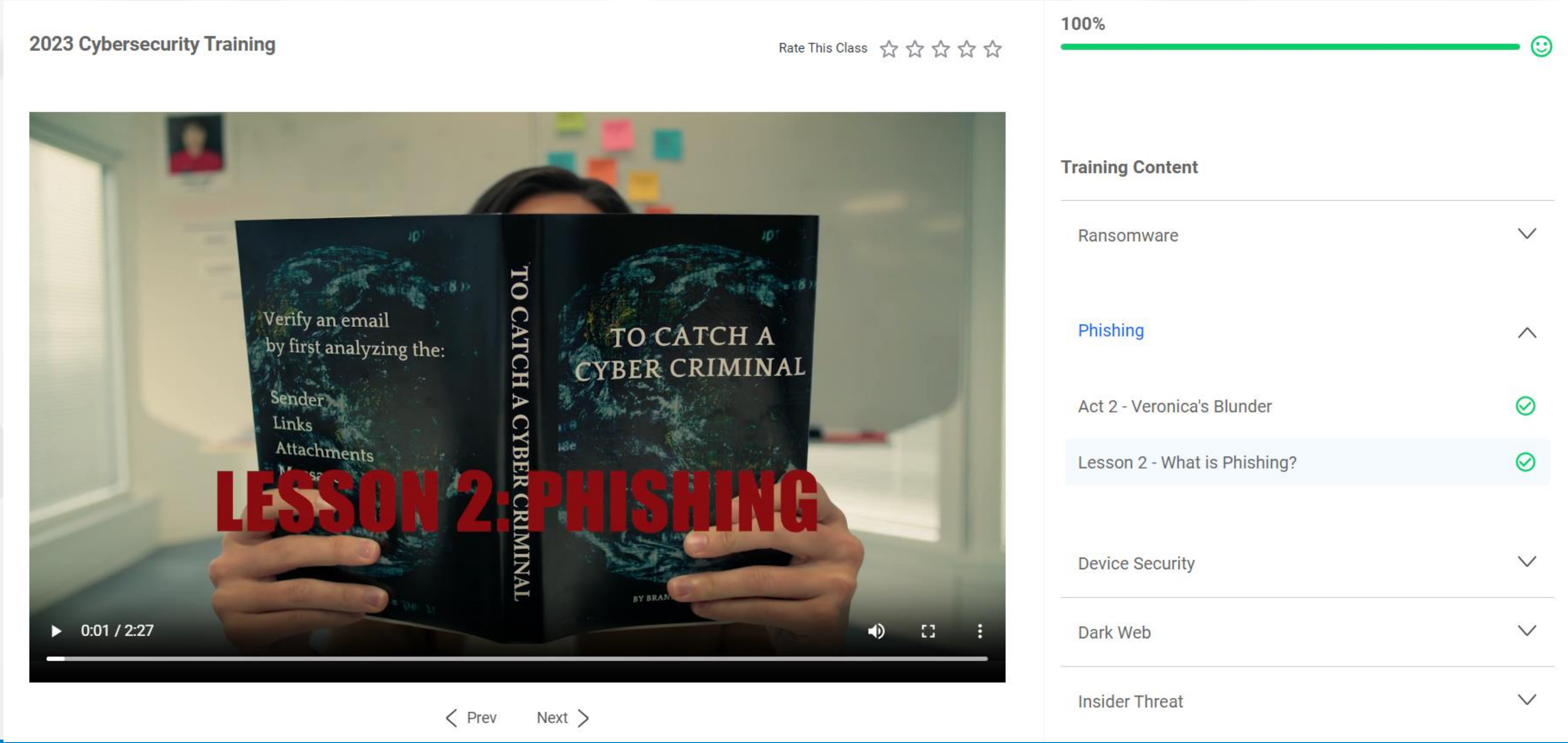
- ✓ **When (not if) a threat gets through, your employee needs to be prepared**
  - What does a Phishing email look like?
  - Is it safe to click on links?
  - Download an attachment?
- ✓ **What is social engineering?**

Cybersecurity Training Approach?

Have staff sit through a PowerPoint?

Provide Books & Reading Material?

Self-paced, Interactive...



2023 Cybersecurity Training

Rate This Class ☆ ☆ ☆ ☆ ☆

100%

Training Content

- Ransomware
- Phishing
  - Act 2 - Veronica's Blunder ✓
  - Lesson 2 - What is Phishing? ✓
- Device Security
- Dark Web
- Insider Threat

Train, Test, and Track

Mandatory Training Courses

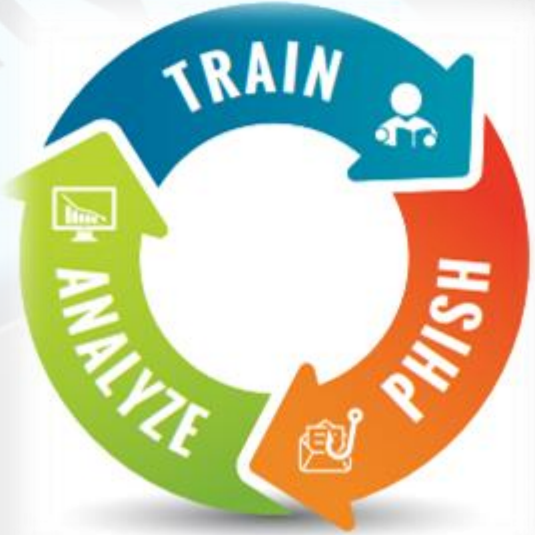
- Self-paced with completion dates
- Online, interactive, trackable
- Small chunks, various subjects overtime

Situational Testing

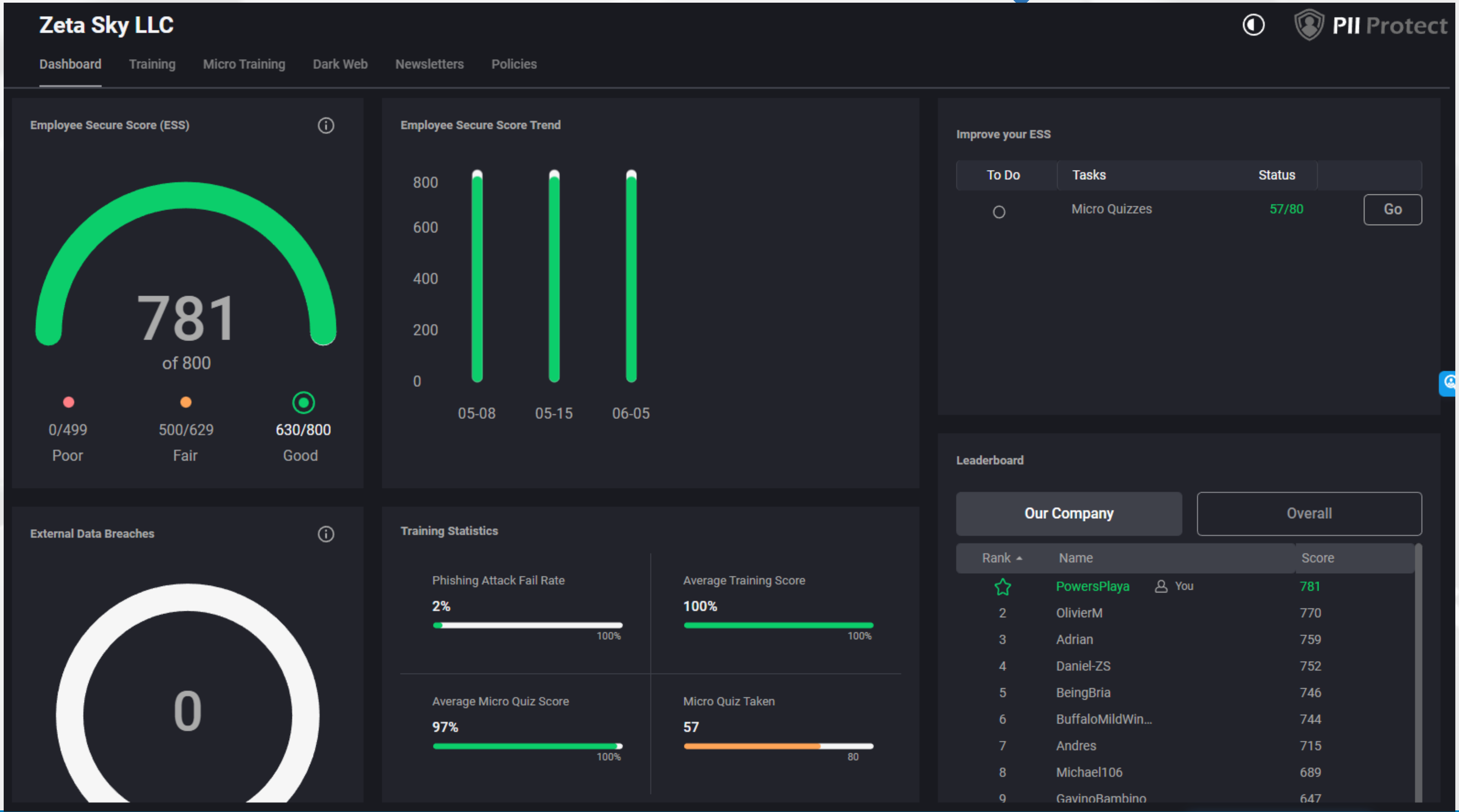
- Simulated, ongoing/random phishing attacks

Report

- Who's completed testing
- Who's clicking on Phishing links
- Who needs additional training



360 Security Awareness Program



Zeta Sky LLC

PII Protect

Dashboard | Training | Micro Training | Dark Web | Newsletters | Policies

Employee Secure Score (ESS)

781
of 800

0/499	500/629	630/800
Poor	Fair	Good

Employee Secure Score Trend

Improve your ESS

To Do	Tasks	Status	
○	Micro Quizzes	57/80	Go

External Data Breaches

0

Training Statistics

Phishing Attack Fail Rate
2%
100%

Average Training Score
100%
100%

Average Micro Quiz Score
97%
100%

Micro Quiz Taken
57
80

Leaderboard

Our Company | Overall

Rank	Name	Score
☆	PowersPlaya You	781
2	OlivierM	770
3	Adrian	759
4	Daniel-ZS	752
5	BeingBria	746
6	BuffaloMildWin...	744
7	Andres	715
8	Michael106	689
9	GavinoBambino	647

So…Where Do You Start?

1. **Conduct a security / vulnerability assessment**
   a. What layers of security to you have in place?
   b. Are they up to date? Who is managing security?
   c. Consider 3rd party penetration/vulnerability testing*
   d. Identify potential gaps and solutions you can implement

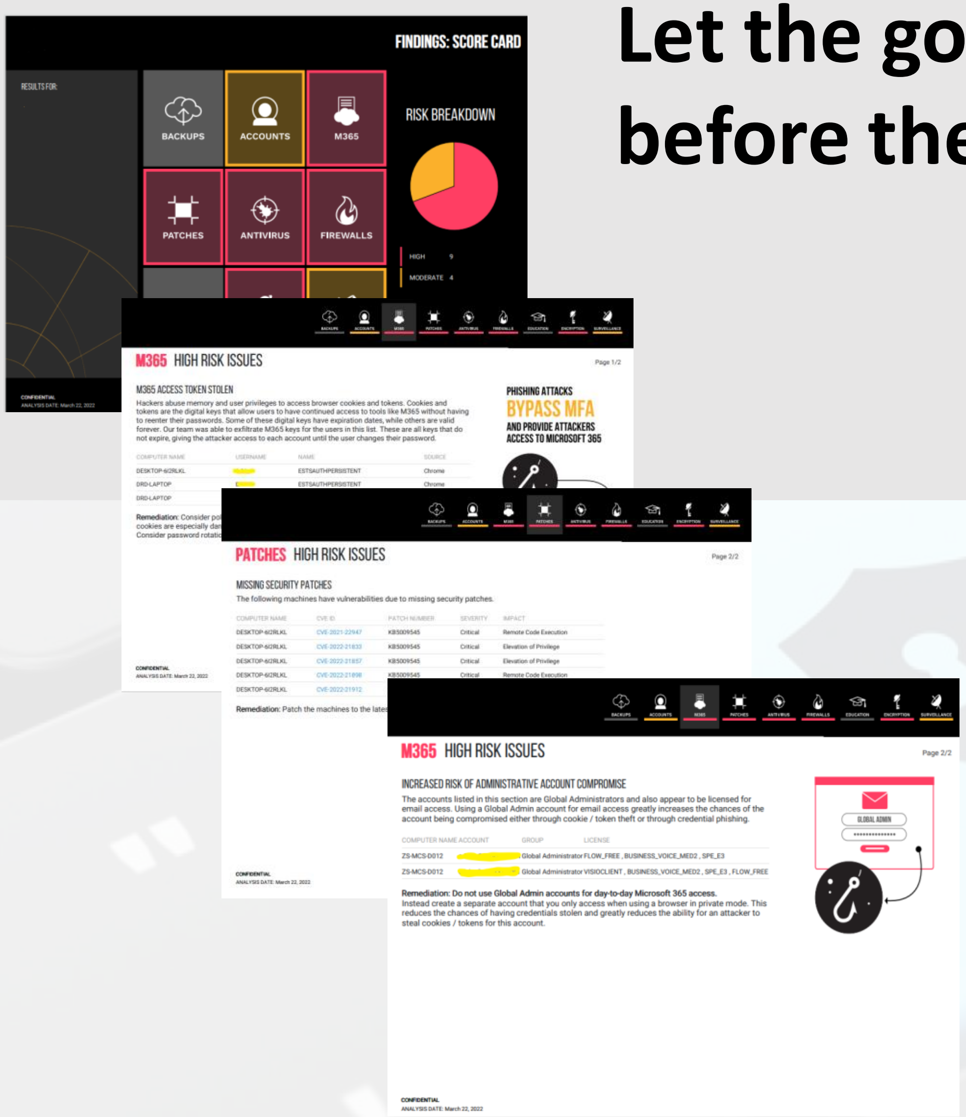
2. **Verify & Test your Backup and Disaster Recovery**
   a. If an attack gets through, can you recover? How quickly?

3. **Strengthen Your Human Firewall!**
   a. Implement a mandatory, easy to use, ongoing cyber awareness training platform for your team.

*Ethical hacking- hire professionals to emulate a cyberattack and discover vulnerabilities and points of entry.

Level 1 Pen Test: Security Test Your Network

Let the good guys find vulnerabilities before the bad guys do…



FINDINGS: SCORE CARD

RESULTS FOR:

CONFIDENTIAL
ANALYSIS DATE: March 22, 2022

M365 HIGH RISK ISSUES

Page 1/2

M365 ACCESS TOKEN STOLEN

Hackers abuse memory and user privileges to access browser cookies and tokens. Cookies and tokens are the digital keys that allow users to have continued access to tools like M365 without having to reenter their passwords. Some of these digital keys have expiration dates, while others are valid forever. Our team was able to exfiltrate M365 keys for the users in this list. These are all keys that do not expire, giving the attacker access to each account until the user changes their password.

COMPUTER NAME	USERNAME	NAME	SOURCE
DESKTOP-6I2RLKL	[redacted]	ESTSAUTHPERSISTENT	Chrome
DRD-LAPTOP	[redacted]	ESTSAUTHPERSISTENT	Chrome
DRD-LAPTOP			

PHISHING ATTACKS
BYPASS MFA
AND PROVIDE ATTACKERS ACCESS TO MICROSOFT 365

Remediation: Consider pol
cookies are especially dan
Consider password rotatio

CONFIDENTIAL
ANALYSIS DATE: March 22, 2022

PATCHES HIGH RISK ISSUES

Page 2/2

MISSING SECURITY PATCHES

The following machines have vulnerabilities due to missing security patches.

COMPUTER NAME	CVE ID	PATCH NUMBER	SEVERITY	IMPACT
DESKTOP-6I2RLKL	CVE-2021-22947	KB5009545	Critical	Remote Code Execution
DESKTOP-6I2RLKL	CVE-2022-21833	KB5009545	Critical	Elevation of Privilege
DESKTOP-6I2RLKL	CVE-2022-21857	KB5009545	Critical	Elevation of Privilege
DESKTOP-6I2RLKL	CVE-2022-21898	KB5009545	Critical	Remote Code Execution
DESKTOP-6I2RLKL	CVE-2022-21912			

Remediation: Patch the machines to the lates

CONFIDENTIAL
ANALYSIS DATE: March 22, 2022

M365 HIGH RISK ISSUES

Page 2/2

INCREASED RISK OF ADMINISTRATIVE ACCOUNT COMPROMISE

The accounts listed in this section are Global Administrators and also appear to be licensed for email access. Using a Global Admin account for email access greatly increases the chances of the account being compromised either through cookie / token theft or through credential phishing.

COMPUTER NAME	ACCOUNT	GROUP	LICENSE
ZS-MCS-D012	[redacted]	Global Administrator	FLOW_FREE , BUSINESS_VOICE_MED2 , SPE_E3
ZS-MCS-D012	[redacted]	Global Administrator	VISIOCLIENT , BUSINESS_VOICE_MED2 , SPE_E3 , FLOW_FREE

Remediation: Do not use Global Admin accounts for day-to-day Microsoft 365 access.
Instead create a separate account that you only access when using a browser in private mode. This reduces the chances of having credentials stolen and greatly reduces the ability for an attacker to steal cookies / tokens for this account.

CONFIDENTIAL
ANALYSIS DATE: March 22, 2022

- Simple to execute, no need to provide any access to your network.
- Simulates a Phishing Attack-
  What would happen if a bad actor get access to a computer?
- Report the findings, vulnerabilities and remediation plan

CyberSecure™ MY BUSINESS

- For SMB Owners/Operators
- Focus on *managing* cybersecurity, not ‘*doing*’ cybersecurity
- 6 Modules, once per week; 50 minutes of live learning
- A worksheet of practical actions to take in between sessions
- ~30 companies in a single cohort
- Ongoing access to a peer community

ZETA SKY
ELEVATING BUSINESS TECHNOLOGY

Cybersecurity Resources

Schedule a Level 1 Security Assessment for YOUR Business.

FREE Cyber Awareness Training Course for your ENTIRE company.

TRAIN
PHISH
ANALYZE

NCA Business Leader Training Course

CyberSecure™
MY BUSINESS

Cybersecurity Resources

Take Advantage of a **FREE** Security Assessment and Guidance for **YOUR** Business

ZETA SKY