UNMASKING THE UNINVITED:

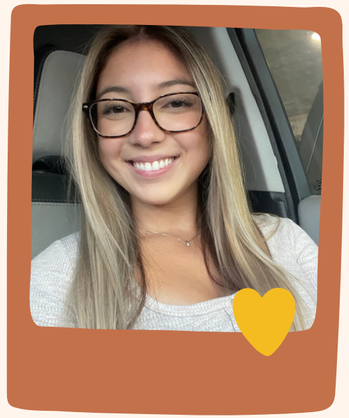
AN EXPLORATION OF COMBATING UNAUTHORIZED NETWORK ACCESS

Our Team

Larnelle Ankunda

Cameron Proulx

Vidushi Singh



Yari Sarduy

Ayomide Adekoya

HAVE YOU EVER DEALT WITH UNAUTHORIZED NETWORK ACCESS OR SCARED THAT YOUR BUSINESS MAY BE NEXT??!

HACKING IS ON THE RISE!!

McLaren Health Care Hack Affected Millions; Lawsuits Pile Up

Michigan Healthcare Provider Faces 7 Federal Lawsuits in Alphv/BlackCat Data Theft

Marianne Kolbasuk McGee (HealthInfoSec) • November 13, 2023

Share Tweet Share Credit Eligible Get Permission

McLaren Health Care is facing seven proposed federal class action lawsuits following a recent data theft affecting nearly 2.2 million patients. (Image: McLaren)

MGM and Caesars hit with class-action lawsuits over Nevada cyberattacks

Five complaints filed with Nevada District Court suggesting operators breached duty of care in not preventing immobilizing hack

Robert Simmons
26/09/2023

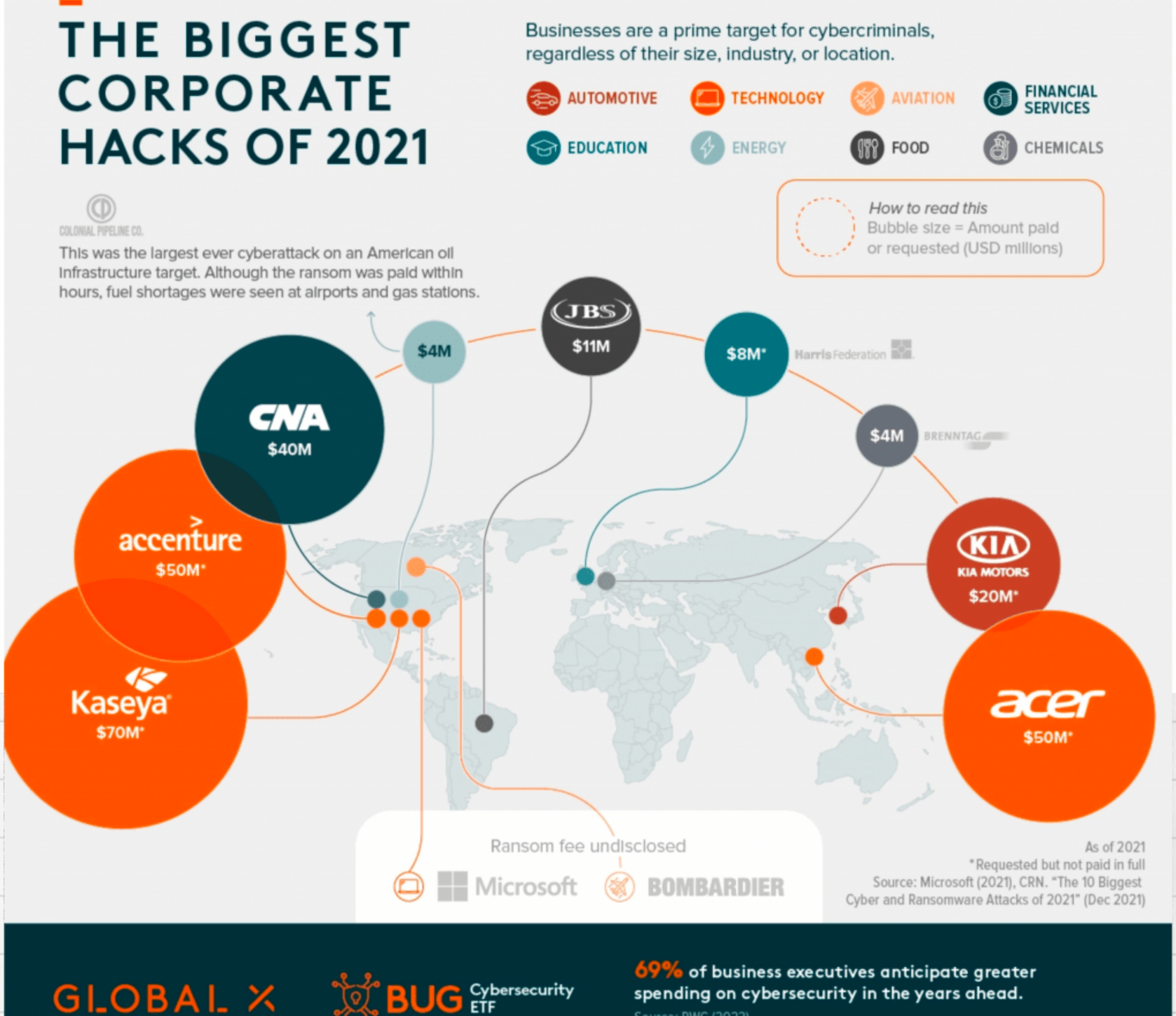
CommonSpirit Health revealed that cybersecurity breach was much larger than initially thought, reaching 100 facilities in 13 states

By **Annie Burky** • Apr 10, 2023 1:30pm

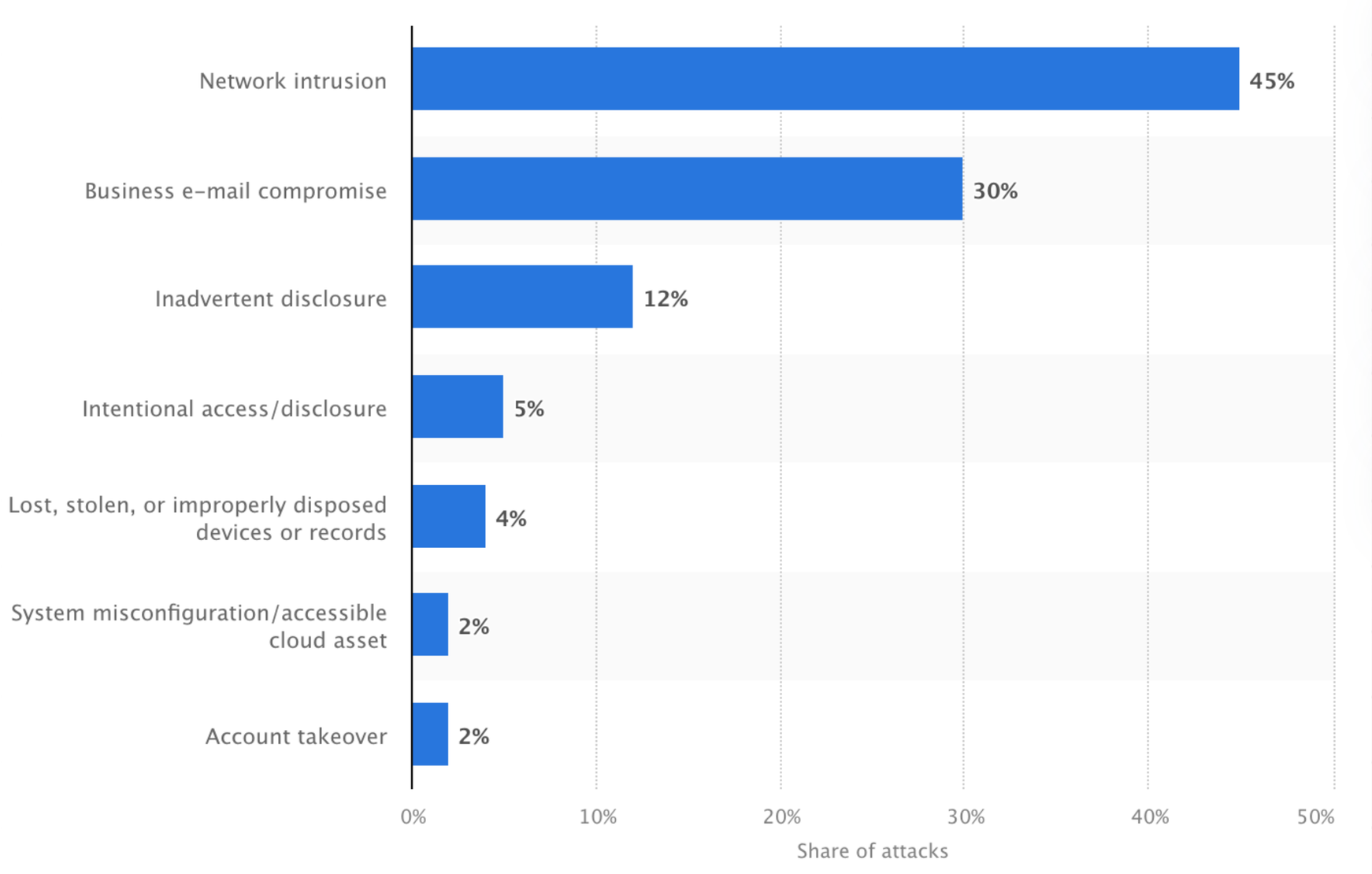
CommonSpirit Health | CHI Health | Virginia Mason Health System | cyberattack

CommonSpirit Health previously said it had engaged law enforcement and outside cybersecurity specialists to aid its forensics investigation of a breach that comprised the data of over 600,000 patients. (Getty Images)

“BUSINESSES ARE A PRIME TARGET”



NETWORK INTRUSIONS ARE THE MAIN CULPRIT



MOST COMMON TYPES OF CYBER ATTACKS EXPERIENCED BY COMPANIES IN THE U.S. 2022

SOURCE: STATISTA.COM

WE CAN HELP YOU!

RISK MITIGATION STRATEGIES

NETWORK SCANNER

- Scans devices on network
- Detects vulnerabilities
- Allows administrators do their job
- Security holes get fixed before they get exploited

FIREWALL

- Barrier between the inside and outside of network
- Monitors incoming and outgoing network traffic
- Analyzes each packet of data
- Prevents attackers from gaining entry

NETWORK SCANNER

Vulnerability Detection:

- Robust scanning capabilities to identify vulnerabilities
- Using a comprehensive vulnerability database to ensure coverage for security threats

Automated Scanning and Scheduling

- Automated scanning processes to regularly check for potential vulnerabilities.
- Scheduling options for scans during non-business hours to minimize disruption

Prioritization and Risk Assessment

- Implementing a risk assessment feature that prioritizes identified vulnerabilities based on severity.
- Provide detailed reports to assist administrators in focusing on critical security holes first.

Integration with Patch Management Systems

- To Streamline the remediation process
- Enable administrators to directly apply patches or updates to fix identified vulnerabilities through a centralized interface.

Anomaly Detection and Behavior Analysis

- Include anomaly detection mechanisms to identify unusual behavior on the network
- Implement behavior analysis algorithms to detect deviations from normal patterns.

User Authentication and Access Control

- Use of strong authentication mechanisms to ensure that only authorized personnel can access and configure the network scanner.

CREATING A NETWORK SCANNER

What it is and how it works

A network scanner is a software tool that scans the network for connected devices. Here's how it works:

- The sending device sends an ARP Request containing the IP Address of the device it wants to communicate with.
- After receiving the broadcast message, the device with the IP address equal to the IP address in the message will send an ARP response containing its MAC address to the sender.

Implementing the network scanner

In our python script, we will follow these steps to design our network scanner:

- Creating an arp request packet which has the target IP address.
- Send packet to the broadcast and receive a response from the target IP address.
- parse the response to get the Mac
- print result

CREATING A FIREWALL PT1

What You'll Need:

- A PC
- A blank CD-R
- At least two Ethernet ports
- Hard drive/ USB thumb drive

Network Design

- Cable modem for internet access
- Internal LAN with workstations, home file server, TiVos, and VOIP adapter
- Public wireless network separated on DMZ network
- Wireless access point on DMZ network
- DMZ network restricted from accessing the LAN without special rules

Make the CD

- Download Devil Linux stable release
- Unzip the downloaded file
- Find and burn the bootcd.iso file to a CD using suitable software

Hardware Setup

- Devil Linux is a 'live' distribution, runs directly from CD-ROM
- Configuration stored on a separate disk (floppy drive or USB thumb drive)
- PC needs a CD-ROM drive, no hard drive required

Boot-up:

- -Connect monitor and keyboard
- Insert boot CD and power up
- Watch for the boot screen, and system will automatically boot

Login:

-Enter 'root' as the username
Press enter for the password
Type 'setup' and press enter to access the setup menu

CREATING A FIREWALL PT2

Congifiguration:

- Navigate setup menu (arrow keys, spacebar)
- Configure basics (hostname, timezone)
- Enable/disable network services (e.g., SSHD, NAMED)
-

Network Setup

- Configure NICs in Networking menu
- Set modules for each NIC
- Configure IP for eth0 (internet-facing NIC)
- Configure additional NICs (e.g., eth1, eth2)
- Set DHCP for local NICs if needed
-

Firewall Configuration:

- Choose DMZ3FW or FW2 in Networking menu based on NICs
- Install basic firewall rules (select 'yes')

DHCP Configuration:

-Adjust DHCP settings in main menu option

Password and Save Configuration::

- Set root password using LoginPW or 'passwd'
- Save configuration changes using 'save-config' or 'save-config' command

COST BENEFIT ANALYSIS

$112,000

CYBERSECURITY ANALYST COST PER YEAR

$9,480,000

NETWORK INTRUSION COST

SOURCES: BUREAU OF LABOR STATISTICS, STATISTA.COM

THANK YOU VERY MUCH!

NETWORK SCANNER

Product Options

- Nessus

Setup Time

- 1 week?

Setup Cost

- $1500?

Maintenance Outlook

- What does IT do to use this on an ongoing basis?

Maintenance Cost

- 10% of IT budget?

Demonstrate knowledge

- explain the benefits of Nessus as a vulnerability scanner versus a network mapper like nmap?

NEXTGEN FIREWALL

Product Options

- Palo Alto
- FortiGate

Setup Time

- 1 week?

Setup Cost

- Fortigate hardware NGFW's cost $1,000-$4,000 for SMB's.
- Installation downtime may cause revenue loss

Maintenance Outlook

- What does IT do to use this on an ongoing basis?

Maintenance Cost

- 10% of IT budget?

Demonstrate knowledge

- explain the benefits of a Next-Generation Firewall (NGFW)