UNMASKING THE UNINVITED:

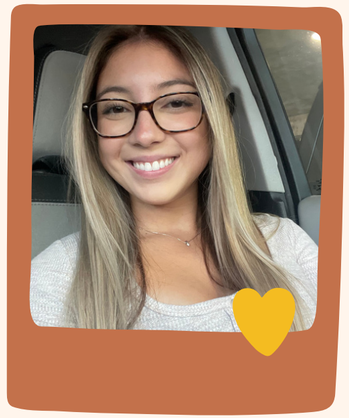
AN EXPLORATION OF COMBATING UNAUTHORIZED NETWORK ACCESS

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

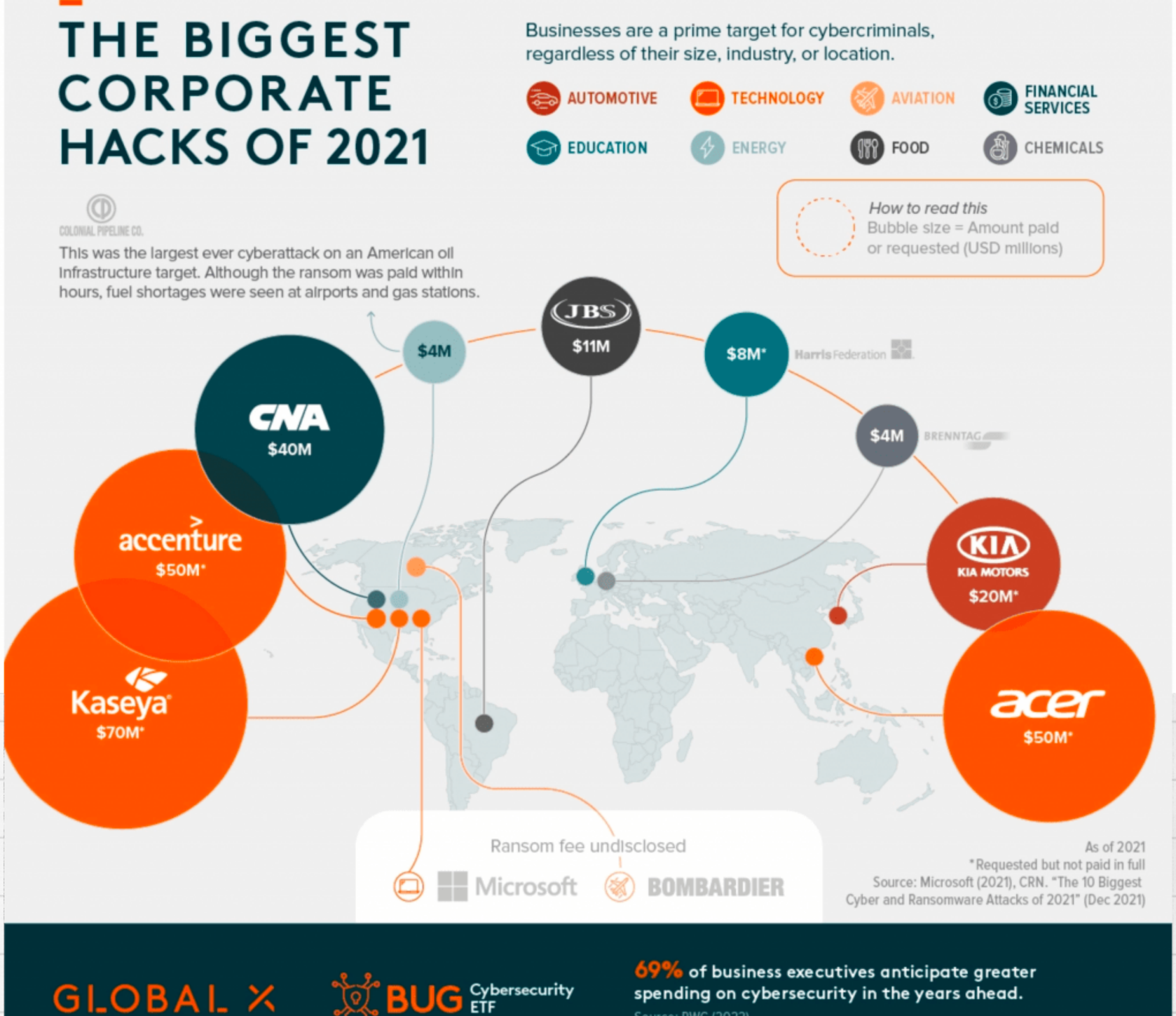
CommonSpirit Health revealed that cybersecurity breach was much larger than initially thought, reaching 100 facilities in 13 states

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

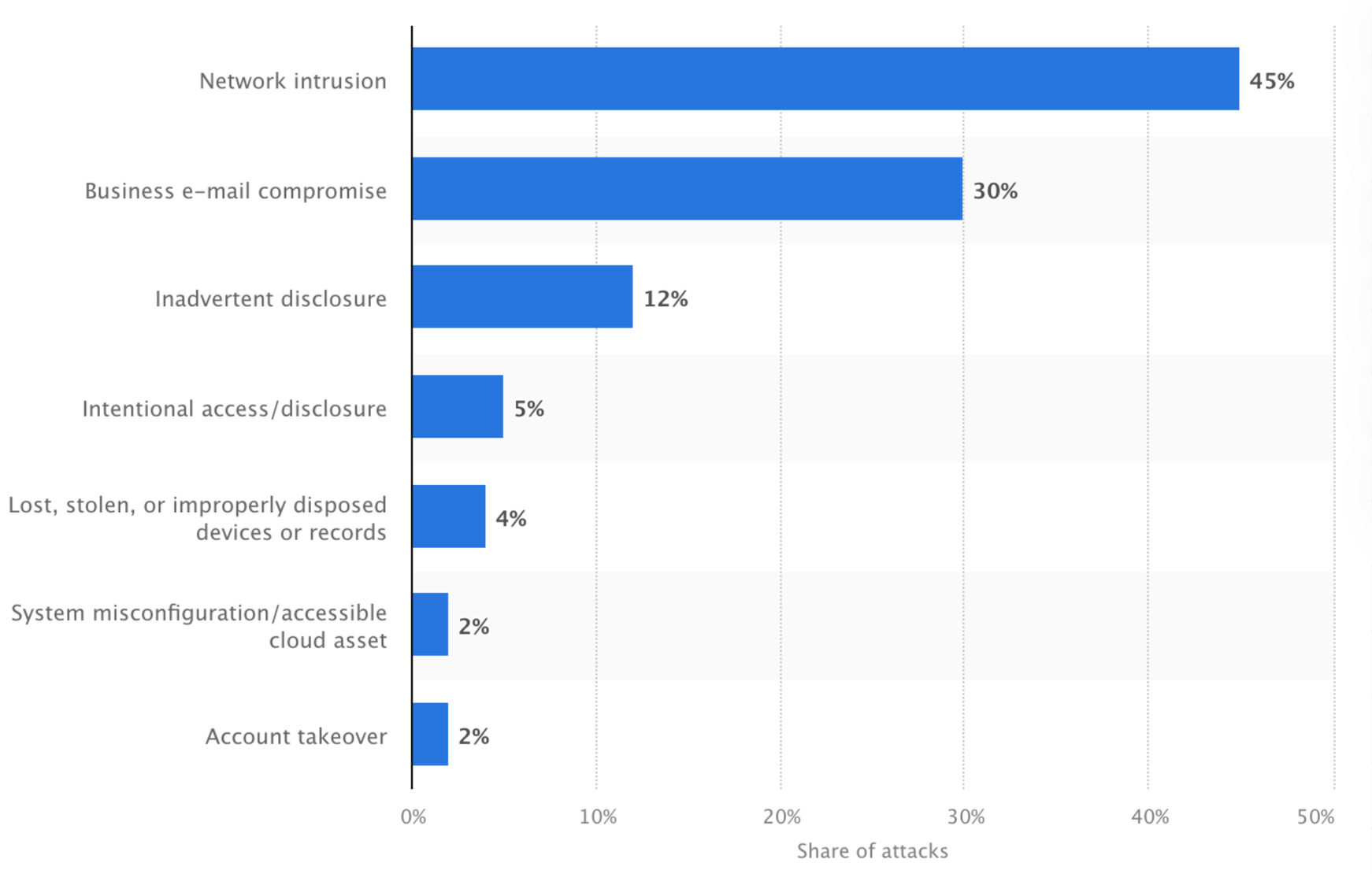
CommonSpirit Health | CHI Health | Virginia Mason Health System | cyberattack

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

Product Options

- Tenable Security Center (Nessus)
  - Ideal for large enterprises
- Rapid7 Nexpose
  - Ideal for SMB's

Setup Time

- Nexpose takes approximately 15 days to install and configure, depending on the complexity of the network

Setup Cost

- Hardware cost to run Nexpose varies. Can run on AWS.
- No network downtime, but may cost take 15 days of IT wages

Maintenance Outlook

- Rapid7 has favorable reviews for their UI and support staff
- Being software-based, Nexpose won't require EOL hardware upgrades

Maintenance Cost

- Expect to spend ~10% of IT budget on cybersecurity
- $20-25/yr per asset. e.g. $6500/yr for 250 network assets

Important Considerations

- Nexpose is an ideal choice because of its intuitive UI, excellent customer support, and leading updates to their CVE list and identification technology

NEXTGEN FIREWALL

Product Options

- Palo Alto
  - Ideal for large enterprises
- Fortinet FortiGate
  - Ideal for SMB's

Setup Time

- Installation may take several days depending on complexity of network and user base

Setup Cost

- FortiGate hardware costs $1,000-$4,000 for SMB's.
- Installation downtime may cause revenue loss

Maintenance Outlook

- FortiGate has leading UI and customer support which reduces maintenance and downtime

Maintenance Cost

- Expect to spend ~10% of IT budget on cybersecurity
- FortiGate licenses cost ~50% of hardware cost per year
- Hardware upgrade every 5 years

Important Considerations

- NGFW's are preferred over traditional firewalls because they combine several security technologies into one platform to combat the latest attack vectors

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 NETWORK FIREWALL PT1

Network Design

- Cable modem for internet access
- Internal LAN with workstations, home file server,
- Public wireless network separated on DMZ network

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 NETWORK FIREWALL PT2

Congifiguration:

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

Firewall Configuration:

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

Network Setup

- Configure NICs in Networking menu. (NICs stands for Network Interface Cards
- Set modules for each NIC
- Configure IP for eth0 (internet-facing NIC)
- Set DHCP for local NICs if needed

DHCP Configuration:

-Adjust DHCP settings in main menu option

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!