SECUREWON
Protecting Possibilities

Prepping for an Event:
Incident Response

What is Cybersecurity?

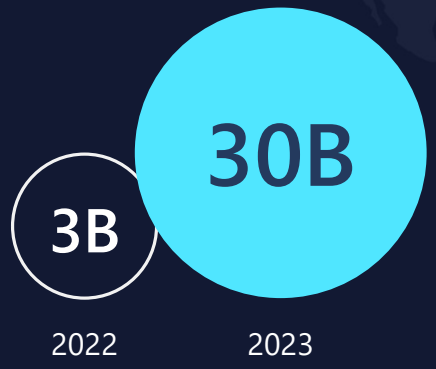
Cybersecurity is the practice of protecting systems, networks and programs from digital attacks.

In real terms, organizations need a comprehensive solution that is built for them to protect its information, reputation, and continuity!

We live in the most complex threat landscape in history

Speed, scale, and sophistication of attacks

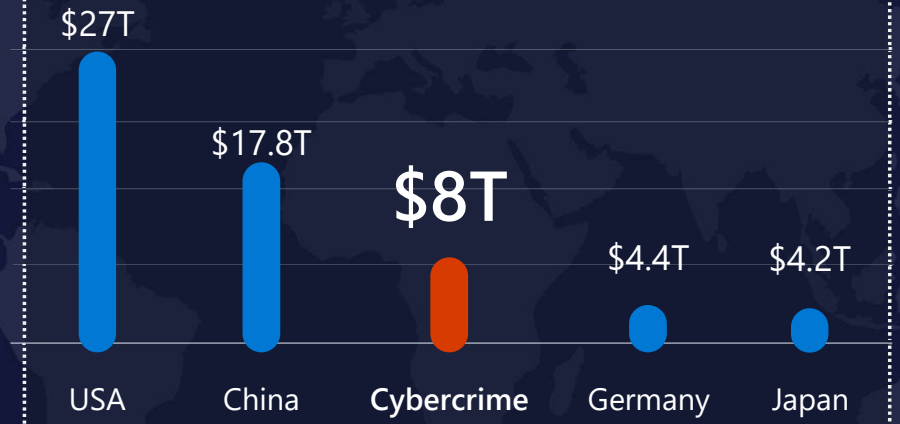
Password attacks per month



Source: Microsoft

Rapidly growing cyber economy

Annual GDP



Source: Statistica

Growing regulatory environment

250

new regulatory updates tracked every day

Source: Microsoft

A Holistic Cybersecurity Solution

People

Engineering
Response Team
Communication
Leadership

Process

Incident Response
Disaster Recovery
Maintenance
Escalation

Technology

MDR
SIEM
BDR
MFA

Cybersecurity Assessments

Data Protection (BCDR)

Vulnerability Management

Cybersecurity Terms

Never use the terms Incident or Breach unless directed to do so by a qualified cybersecurity or forensic professionals.

Attack

An attempt to bypass security. There are millions of events per second.

Event

An event bypassed one ore more levels of security but did not require human intervention to resolve.

Incident

An incident bypassed one or more levels of security, required human intervention to correct, but did not access information.

Breach

An event bypassed one ore more levels of security and modified, deleted, extracted, or read data

Who are these Bad Actors?

Insider Threats

32%

Nation States

< 2%

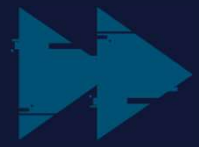
Organized Crime

65%

How do they get paid?

There are three common methods for Bad Actors revenue:

- Ransom: *Where a business will pay for the restoration of their information*
- Extortion: *Where a business will pay to stop the release of their information*
- Data Sale: Where the bad actors will sell your information on the ‘dark web’



Common Access Entry Points

Bad Actors have several methods to access company data!

Environment

- Vulnerabilities (17%)
- Misconfiguration
- Unpatched Systems
- 3rd Party Breach

Human Element

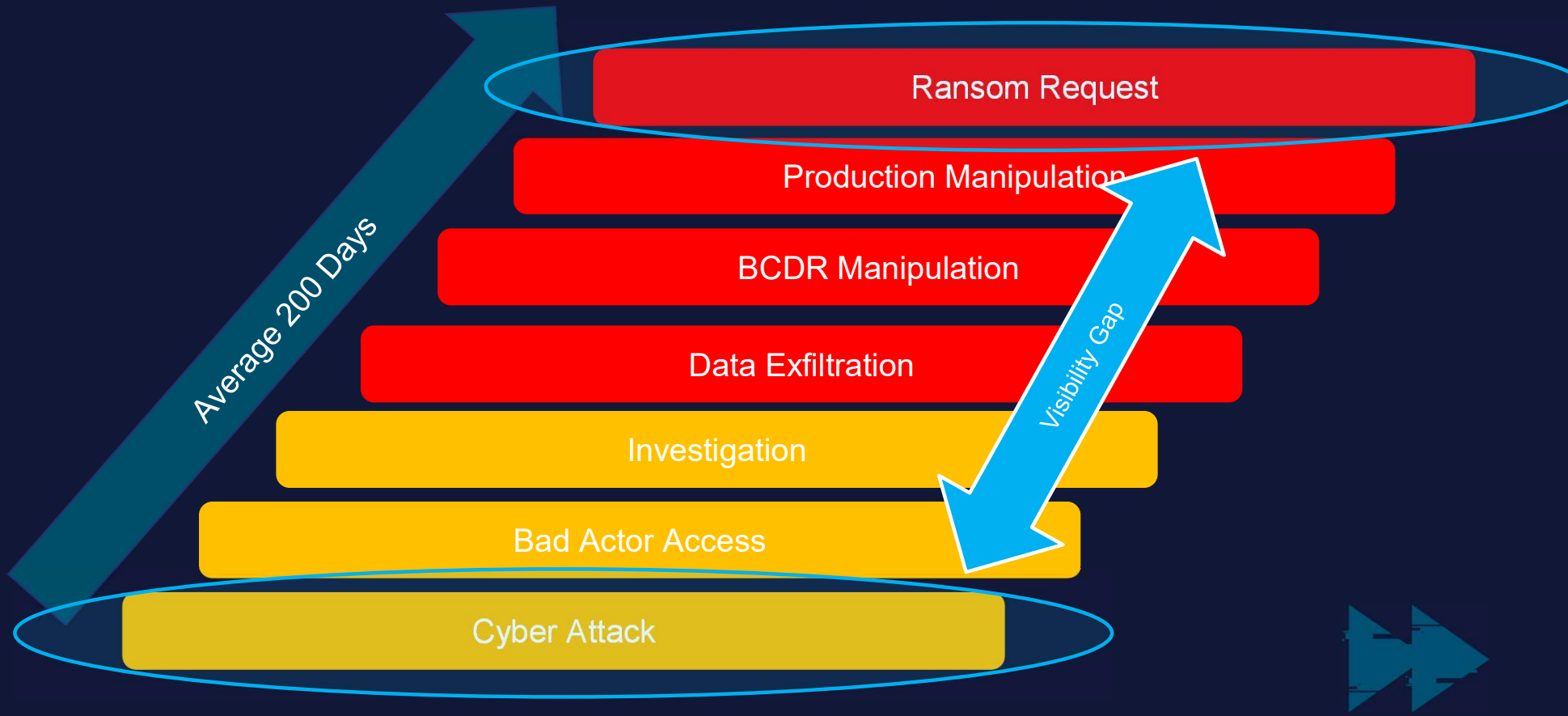
- Credentials (38%)
- Phishing (17%)
- Physical Security Challenges
- Social Engineering

68%

*Excludes Privilege Misuse

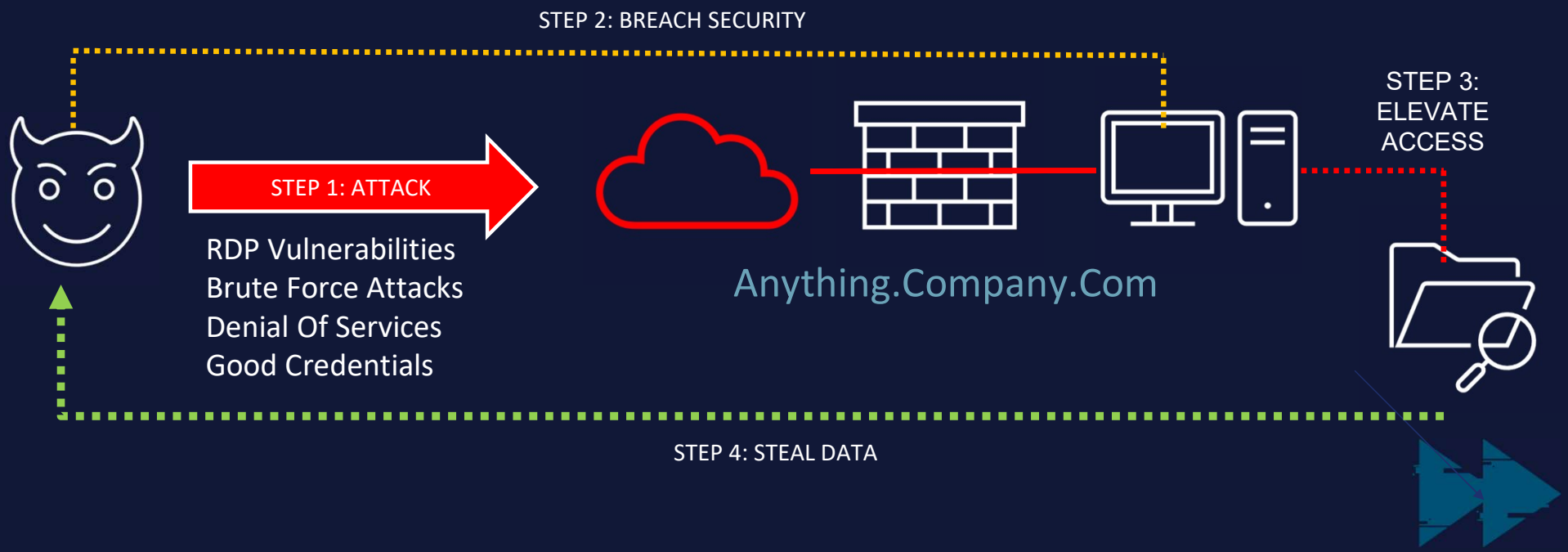
*2024 Verizon DBIR Report

Gaining Access is just the start



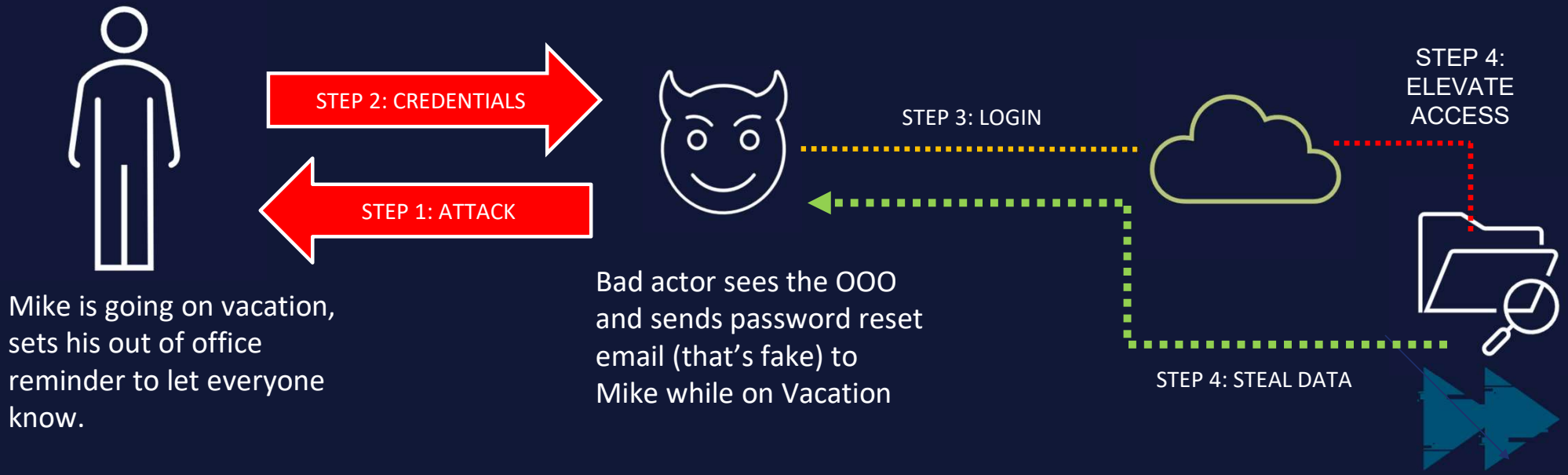
Environment Issue: Exposed System

Situation: Company A uses a common technology for employees to access services inside their network.



Human Error: Social Engineering

Situation: Company A uses Microsoft 365 for Email and SharePoint. They have MFA enabled.



Important Message from Karen Lynch, CEO of CVS

Dear Curtis,

I hope this email finds you well. I wanted to reach out to you personally to inform you of some important updates regarding our company.

As you may know, CVS is committed to providing the best possible healthcare services to our customers. In order to continue to do so, we have recently made some changes to our internal systems and processes.

As a valued member of our team, we need your help to ensure that these changes are implemented smoothly. Please click on the link below to access our new system and complete the necessary training:

http://www.cvs-training.com

If you have any questions or concerns, please do not hesitate to reach out to me directly.

Thank you for your continued dedication to CVS.

Best regards,

Karen Lynch

CEO, CVS Health

Email: klynch@cvs.com

Phone: (555) 123-4567

So how do we protect ourselves?

People

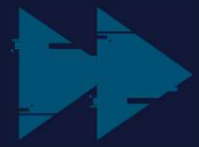
Process

Technology

Technology: A Layered Defense

Business Email Compromise

- Mike, a well-known power user at your company, just called you and mentioned he received an email yesterday that prompted them to log into the network.
- Mike didn’t think anything of it until today, when they realized something seemed odd about it.



Questions/Discussion

What are the first 2-3 things you do?

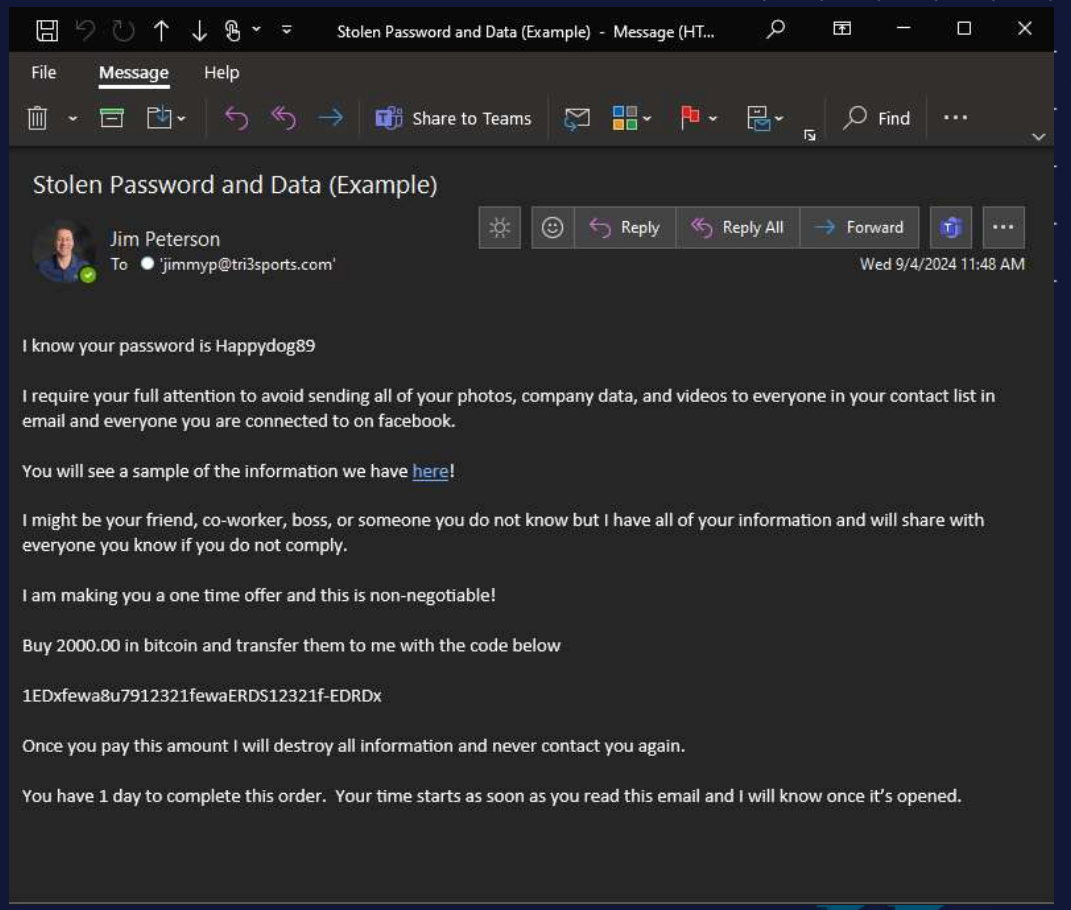
- Contact IT Team or Service Provider
- Isolate Mike's Computer and Access from the Network
- Investigate and Assess

How do you validate that an actual incident has occurred?

- Review Logs and Alerts
- Review User / Admin Account Changes
- Conduct a Network or Security Scan
- Consult with an Expert

Extortion

- A user in your company who managed sensitive information receives this email.
- Where do you start?
  - Enact IRP Contact Process
  - Investigate and Assess



Ransomware

- Turns out the extortion email was just a distraction (miss direction)
- Other machines are now popping up with this bitcoin ransom message
- What do you do?

- Start IRP and BCDR
- Initialize Containment
- Preserve Environment
- Investigate and Assess

Wire Transfer

- Your team finally starts to recover from the ransomware attack, when the client's accounting lead enters the room.
- Exasperated, they report, "While we were down, it looks like there were 4 wires sent from our account totaling almost $100,000."
- What do you do now?

- Start Incident Response Plan
- Contact Banking Center
- Investigate and Assess
- Communicate Processes

Questions/Discussion

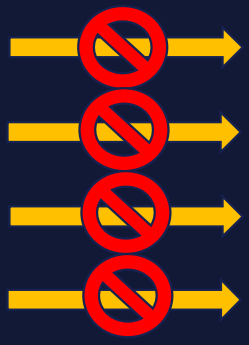
- ✓ What do you communicate to your staff?
- ✓ What do you communicate to your clients / vendors?
- ✓ Do you pay the extortion request?
- ✓ Do you choose to pay the ransom?
- ✓ How do you relieve the stress on your team?
- ✓ How has your message to staff and clients been modified as the situation changed?

Foundation: Six Core Cybersecurity Requirements

- *IRP: Incident Response Plan*
- *EDR / MDR: Endpoint or Managed Detect and Response*
- *MFA: Multi Factor Authentication*
- *SAT: Security Awareness Training*
- *SIEM & SOC: Security Information and Event Management*
- *BCDR: Business Continuity / Disaster Recovery*

When Bad Actors Engage a Prepared Environment

Fake Email Attack
Password Theft
General Exploits
Data Ransom



Security Awareness Training
Multi-Factor Authentication
Assessments + Patching
BCDR

Wrapping it up!

Building a comprehensive cyber strategy is critical to ensuring your business-critical data is always protected!

Everyone is a Target

Ability and willingness to pay outweighs business size.

Build a Layered Defense

There is no magic bullet for cyber protection. Layers of solutions provide the best defense.

Know Your Risks

Building a great protection strategy starts with knowing your businesses individual risks.

SECUREWON

Protecting Possibilities

Thank You!