

CYBER RESILIENCE 101

SURVIVING A 21-DAY CYBER ATTACK



CYBER RESILIENCE 101

AGENDA

- 1 Current State of Cybersecurity
- 2 Five Steps of Cyber Resilience
- 3 Plain English Simple Plan







\$1.5 MILLION

AVG RANSOMWARE PAYOUT IN 2023

\$4.35 MILLION

GLOBAL AVG COST OF A DATA BREACH
IN 2023

Source: <https://www.cobalt.io/blog/cybersecurity-statistics-2024>

\$9.5 TRILLION

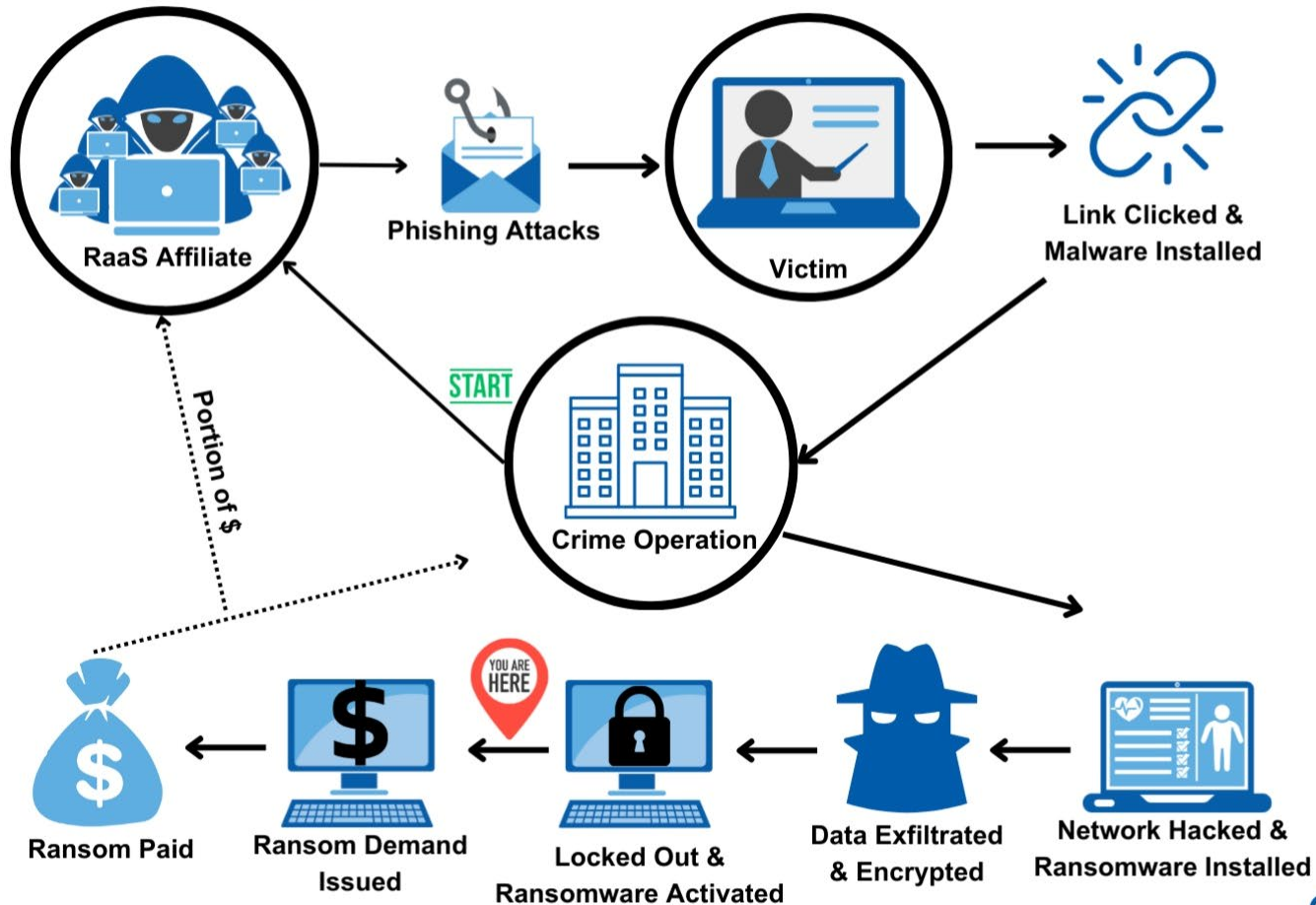
COST OF CYBERCRIME IN 2024

\$13.8 TRILLION BY 2028

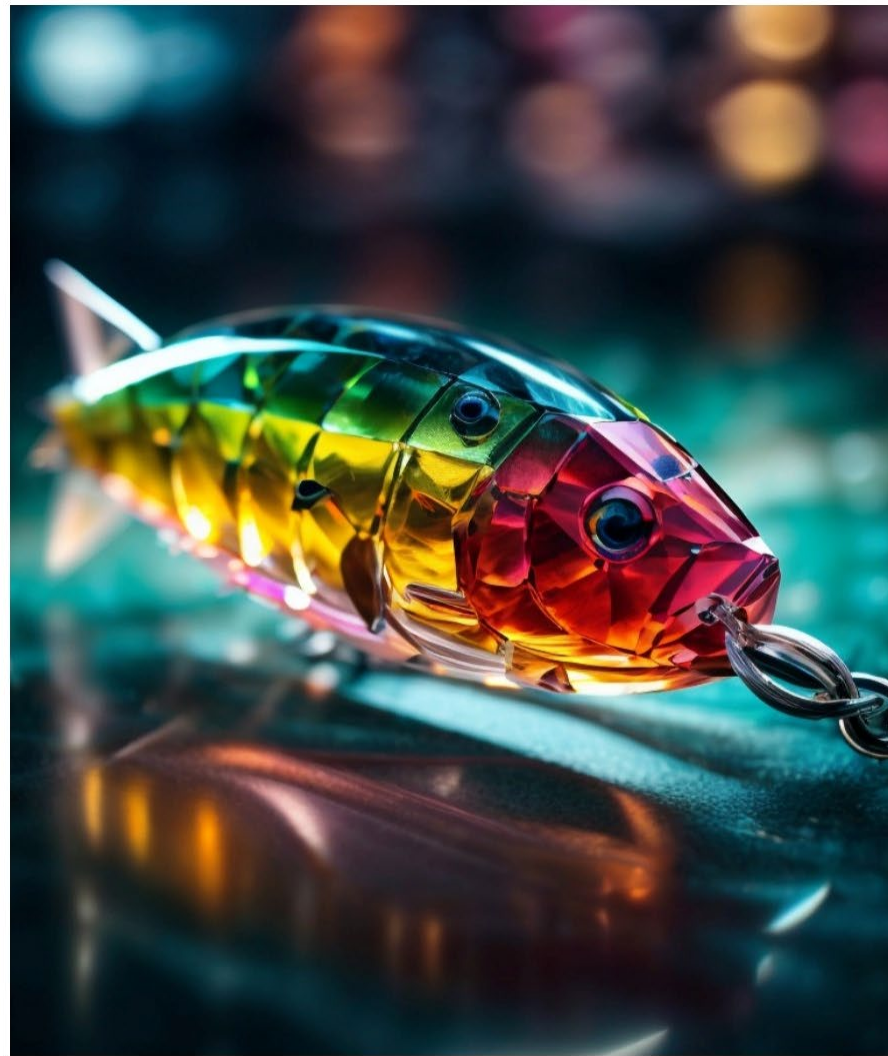
RANSOMWARE



How the RaaS Model Works



PHISHING



THE PHISHING PANDEMIC

CYBER ATTACKS BEGIN WITH PHISHING EMAILS

91%

1 IN 5 EMPLOYEES CLICK ON PHISHING EMAILS

19.8%



AI: ADVANCING CYBERCRIME

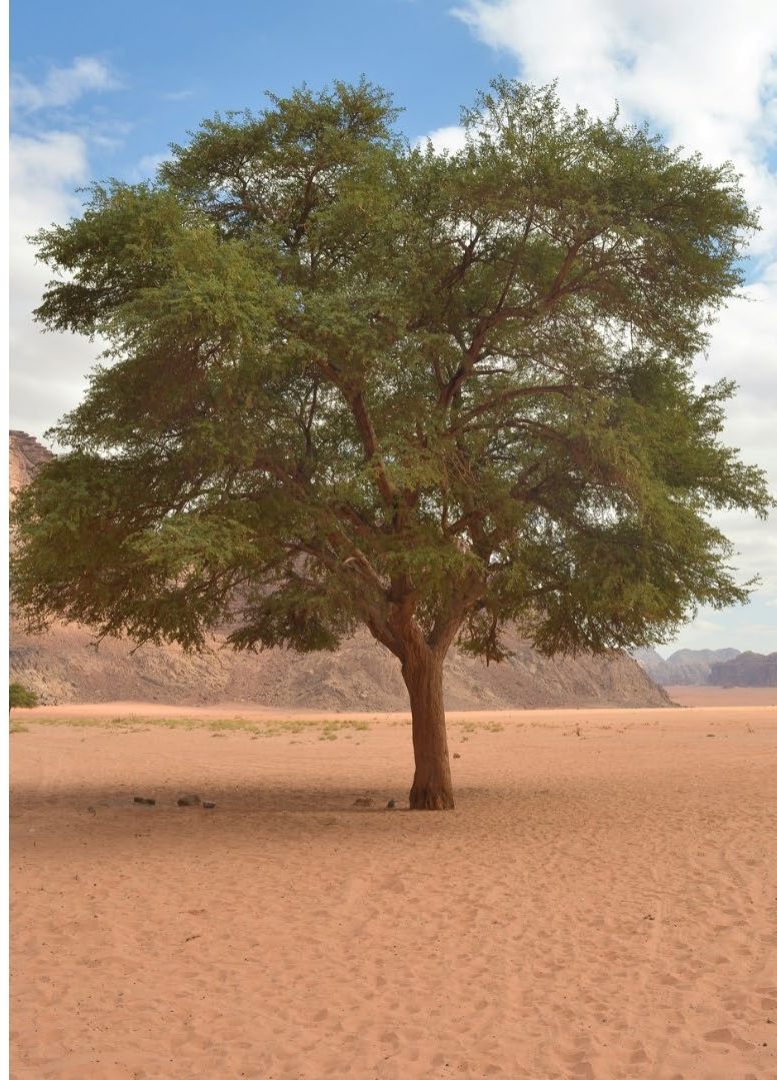




HOW DO WE REACT IN PANIC MODE?

- Fight.
- Flight.
- Cry for help.
- Play dead.
- There is a better way!

CYBER RESILIENCE



A Formula for Cyber Resilience



**Prepare/
Identify**



Protect



Detect



Respond



Recover

Cybersecurity (Elements 1-3)

1. Identify, assess, and manage the risks
2. Protect information and systems
3. Detect anomalies/cybersecurity incidents

Phase 1

Technology

Business Continuity (Elements 4 & 5)

4. Respond with Proven Capabilities
5. Recover Via Incident Management Plan

Phase 2

People and Processes

PREPARE/IDENTIFY

Purpose: Assess Risks and Prioritize Protection

- Document Information Flows
- Establish Policies, Roles and Responsibilities
- Identify and Categorize Important Assets
- Perform an Assessment

Across all infrastructure

Against all known security vulnerabilities



Possible scenarios	Primary workspaces	Primary systems network	Cloud	Data bases and backups	Third party vulnerability
Malware					
Virus	High	Moderate	Moderate	Low	Low
Ransomware	High	High	Moderate	High	High
Phishing	High	Moderate	High	High	High
Crypto Lock	High	High	High	Moderate	High
Communications					
Loss of Vendor Service	Low	High	Low	High	Moderate
Loss of Voice Service	Low	Low	Low	High	Moderate
Loss of Cellular Service	Low	Low	Low	Moderate	Moderate
Loss of Data Transmissions	Low	High	Low	High	Moderate
Router / Hub Failure / Firewall	Low	High	Low	High	Moderate
Overloaded: Performance failure	Low	High	Low	High	Moderate
IT Processing					
Software failure	Low	High	Moderate	Low	Moderate
Infrastructure damaged	Low	High	Low	High	Moderate
Mainframe failure	Low	High	Low	High	Moderate
Server failure	Low	High	Low	High	Moderate
Router failure	Low	High	Low	High	Moderate
Hubs Failure	Low	High	Low	High	Moderate
Utilities and Environment					

Risk Classification:

-  Low
-  Moderate
-  High

PREPARE/IDENTIFY

- Map Your Technology Assets
 - Software, Equipment
 - Devices, Workstations, Servers, IoT, Mobile
 - Data, Backups
- Where are they?
 - On premises, In the Cloud, Hybrid
- How are they connected?
- Are there interdependencies?
- Controls and protections in place?



BUSINESS IMPACT ANALYSIS (BIA)

Determine Business Processes

Impacts of Disruption

Recovery Criticality

Identify Resource Requirements/Dependencies

Identify Recovery Priorities

Google: NIST BIA Template

Email rafe@comtechnc.com for a simplified Excel template

PREPARE/IDENTIFY

- Include Leadership As Part of the Team
- Align Operations and IT
 - Relative to cyber risk and management
 - Encourage a cultural change in employee behavior
- Improve Visibility and Understanding of Information Systems
 - Asset and network mapping
 - Include vendor relationships
- Make Users Cyber Aware
 - Ongoing education
 - Best practices
- Ensure Backup Strategies Are In Place



PROTECT

- GOAL: Reduce the Probability and Impact of a Successful Cyber Attack
- Implement Safeguards, Controls, Processes and Policies
- Manage Access to Assets and Information



Protect

PROTECT

- Protected Against the Latest Threats?
- Disjointed Products/Tools?
- Real-time Visibility of All Assets?
- Automated Enforcement?
- What to Do When Something Seems Wrong?



Protect



PROTECT WHAT?

- Protect and Secure All Technology Assets
- Website and Online Users
- Business-Critical Systems
- Endpoints
- Mobile Workforce
- Supply Chain, Vendors

2



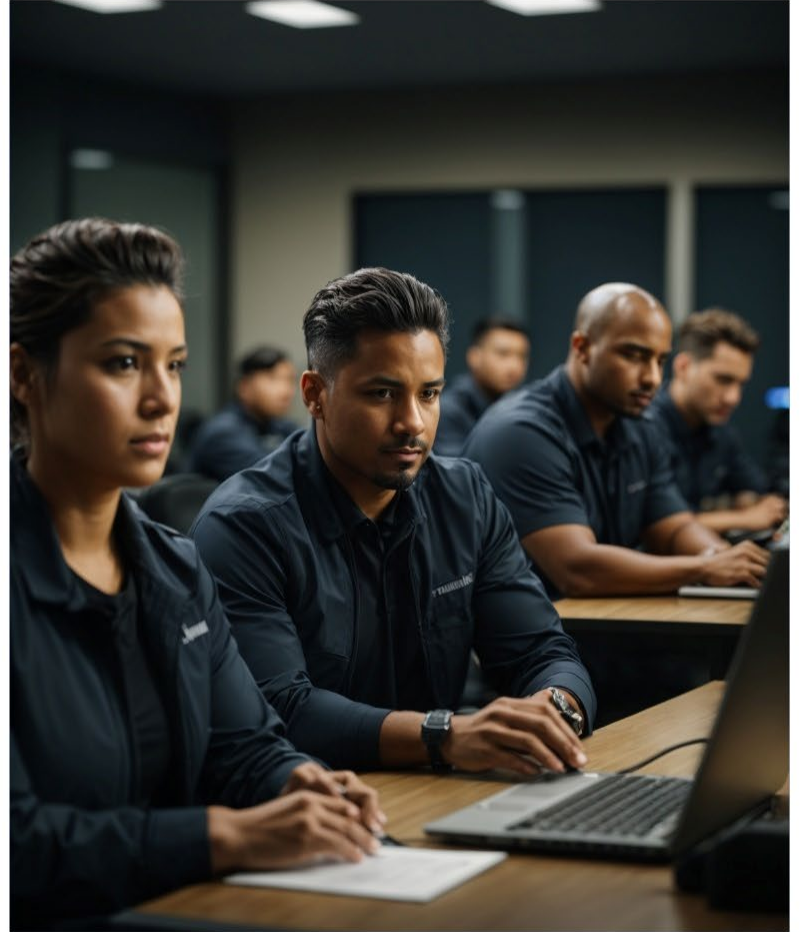
Protect



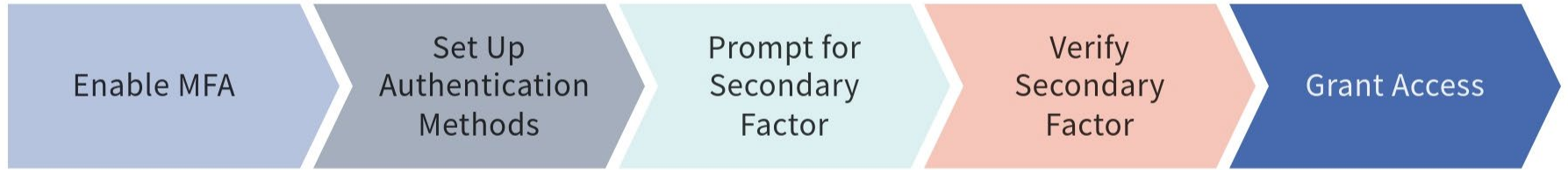
PRACTICAL TIPS: LEAST PRIVILEGED ACCESS



PRACTICAL TIPS: STAFF TRAINING



PRACTICAL TIPS: MULTI-FACTOR AUTHENTICATION



PROTECT: 7 WARNING SIGNS AN EMPLOYEE HAS GONE ROGUE

- Unexpectedly Fails Background Check
- Says Past Employers Didn't Trust Him
- Knows Information He Shouldn't
- Brags He Can Hack a Coworker or Company System
- Switches Screens Away From Company Assets As You Walk Up
- Never Takes a Vacation
- Leaves the Company Angry

Source: <https://www.csoonline.com/article/290515/7-warning-signs-rogue-employees.html>



Protect

THE HUMAN FIREWALL

First Line of Defense

Security-Conscious Culture

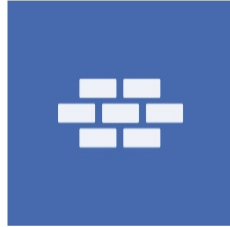
Continuous Training



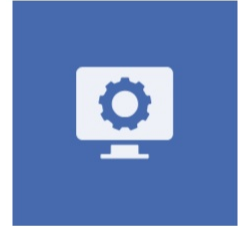
MOVING TO THE CLOUD DOES NOT MEAN YOU OFFLOADED YOUR CYBERSECURITY RESPONSIBILITIES



Install Endpoint Protection



Enable Firewalls



Patch and Update

DETECT

- Identify an Attack Rapidly
- Ensure an Incident Response Plan is in Place
- Assess Affected Systems. How Fast Can You Contain the Attack?



Detect



**\$9.5
TRILLION**

2024 Predicted
Cost of Cybercrime

**21
DAYS**

Average Downtime



CYBER INCIDENT COST FOR A SMALL BUSINESS

Breach Response	\$180,000
Cyber Extortion	\$225,000
Law Firm Retainer	\$25,000
Lost Data Indexing	\$100,000
Digital Asset Restoration	\$200,000
Business Interruption and Extra Expenses	\$400,000
Regulatory Defense and Penalties	\$400,000
Network and Information Security Liability	\$500,000

TOTAL COST \$2,030,000



**\$1.5
MILLION**

Average Ransomware
Payment

**\$4.3
MILLION**

Average Cost of a
Ransomware Event





ZERO TRUST: THE NEW NORMAL



ZERO TRUST

Trust, But Verify

Traditional Approach

Never Trust, Always Verify

Zero Trust Approach

ZERO TRUST ASSUMES BREACH


- Security Framework
- Least Privilege Access




PRACTICAL TIPS: ZERO TRUST CYBERSECURITY BUNDLE

Look for IT providers that offer a Zero Trust bundle.


Cyber Armor Highlights




Zero-Trust Strategy layers multiple protections to provide defense against modern threats. Continuous verification of applications and controls keep systems safe.




24/7 Monitoring by a live security operation center (SOC). If a security event is detected on critical assets, action can be taken to isolate or remediate the threat.




Ransomware Detection and Isolation
We use special detection software that identifies active ransomware activity. It stops the process and isolates the computer from the network.




Application Controls for installing & running programs. By locking down the systems to only allowed programs and processes. If a program can't execute then the threat level is greatly reduced.




Microsoft 365 Risk Watch includes SOC monitoring for threats in your Office 365 cloud. Unusual activity, forwarding rules, international logins and more are monitored.




Ring Fencing puts a fence around your applications and data so hackers or malware can not access them in an unauthorized manner.



SIEM advanced logging for firewalls, servers and Office 365 meets insurance and compliance requirements.



Password Manager company managed credentials are a challenge to maintain. Our password manager solves this nagging problem.



Employee CyberSecurity Training
Human error is the primary cause of cybersecurity events. A properly trained staff helps eliminate errors.



RESPOND

Detection is no good without a timely response!

DETECTION = TECHNOLOGY

RESPONSE = PEOPLE AND PROCESSES



INCIDENT RESPONSE PLAN

INCIDENT RESPONSE PLAN

- A plan to handle cybersecurity incidents quickly and effectively.
- Goal: Limit damage, reduce downtime, and protect your business.
- Essential for minimizing risks from cyber threats.



Respond

INCIDENT RESPONSE STEPS

- **Prepare:** Have a plan in place before an attack happens.
- **Identify:** Detect the problem quickly.
- **Contain:** Stop the spread to protect the rest of the business.
- **Recover:** Get back to business as fast as possible.



WHY PREPARATION MATTERS

- Train your team so they know what to do.
- Have backups and tools ready.
- Practice response scenarios to avoid confusion during a real event.



CONTAINMENT: STOPPING THE SPREAD

- When an incident happens, act fast to isolate the issue.
- Keeping it from spreading minimizes damage to operations.



RECOVERY AND LEARNING

- Restore operations and systems quickly.
- Learn from the event to improve your defenses and response.
- Continuous improvement makes your business more resilient.





BUSINESS CONTINUITY

**A CYBERATTACK IS NOT
JUST AN IT PROBLEM!**

REPUTATION/CRISIS MANAGEMENT



- Communications
 - Media
 - Legal
 - Internal
- Spokesperson
 - Pre-assigned
 - Trained
 - Knowledgeable

RECOVER

Restoring Data and Services



Recover

PRIORITIZATION

Data Backups

Data Recovery

Returning to Normal Operations - What to Restore First



RTC = RECOVERY TIME CAPABILITY

RPC = RECOVERY POINT CAPABILITY

VCIO = CHIEF INFORMATION OFFICER

LESSONS LEARNED

CyberHero Academy



**Training Cyberheroes to
protect Small Businesses
against the Hackers.**

- The CyberHero Academy Training is a FREE in-person cybersecurity training for all staff. ComTech will come to you to train your staff on items such as:
 - How to Identify Threats
 - Password Security Best Practices
 - How to Best Protect Your Company Data
 - Safe Web Browsing
 - Best Practices for Safety on Mobile Devices & Social Media
 - And More!

Register at: www.comtechnc.com/cyberhero-academy

PLAIN ENGLISH TAKEAWAYS

1 Identify

What's Important?

Where is it?

2 Protect

ZERO Trust Framework Checks The Boxes

3 Detect

Identify and Contain Attacks Quickly

4 Respond

Pick Your Quarterback in Advance.

Have a Plan to Continue Business Operations

5 Recover

Know Your RTC and RPC

Lessons Learned





RAFE MARTIN



comtechnc.com



336-338-7328



rafe@comtechnc.com



Book a Meeting at www.rafe365.com