MVP Network Consulting
Technology That Works.

The First 24 Hours After a Cyberattack or Disaster—What to Do

A 24-Hour Response Plan for Organizations

MVP Network Consulting
Technology That Works.

Imagine this:

It’s 2AM.
Your phone rings.
Your company’s network is down.
Ransomware has locked every file.
What you do in the next 24 hours will decide if your business survives-or becomes another statistic?

MVP Network Consulting
Technology That Works.

- Every 11 seconds, a business is hit by ransomware.
- 60% of small businesses close within 6 months of a major cyberattack.
- Average breach goes undetected for 204 days—but **your response in the first day is what matters most.**

MVP Network Consulting
Technology That Works.

Meet Ikram Massabini

CEO of MVP Network Consulting

25 Years of IT Experience

Expert IT Security Consultant

HIPAA Consultant & Auditor

Security Certifications

BS in Electronic Engineering

Get in Touch

Connect with Ikram at:

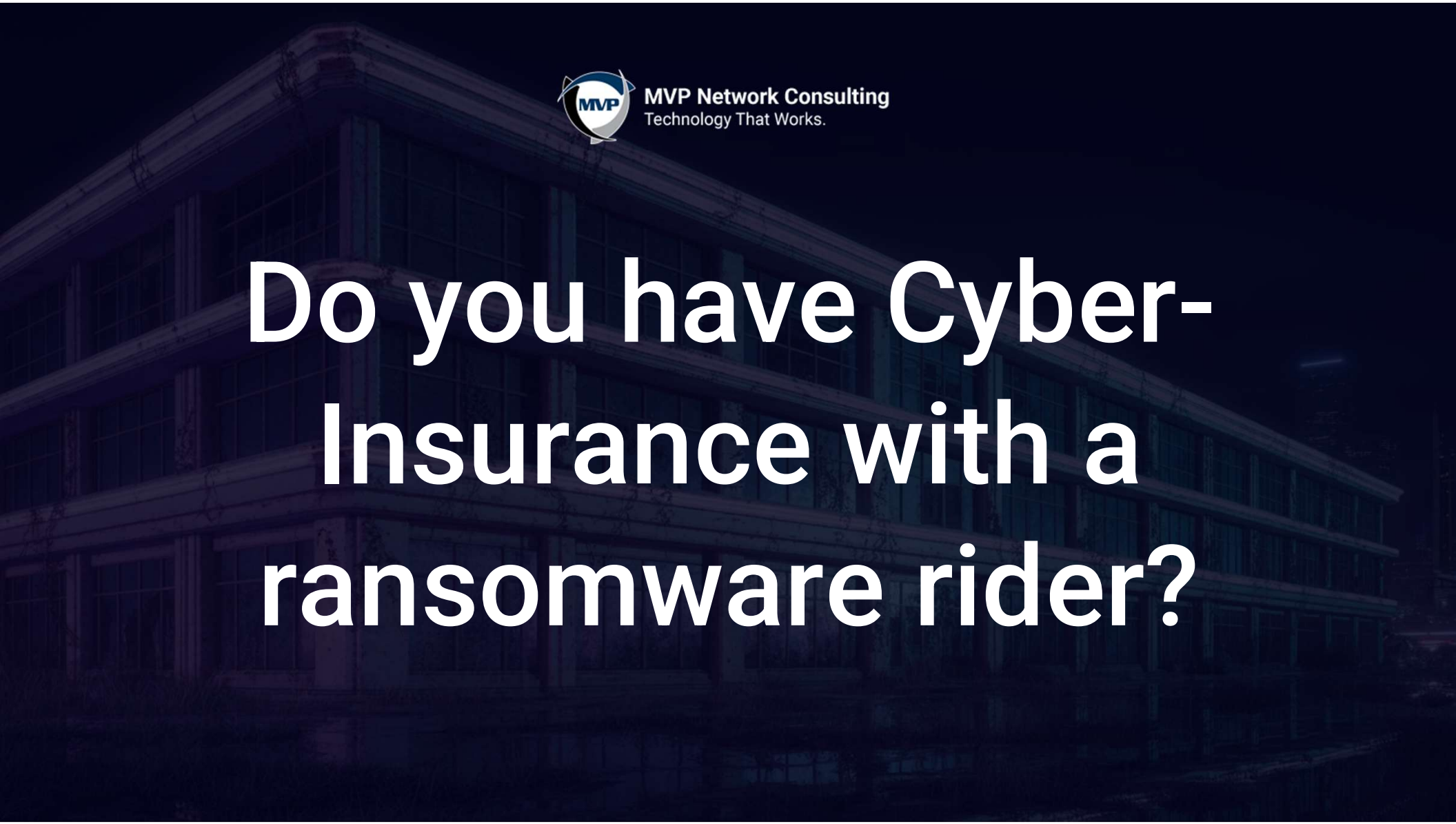
ikram@mvpworks.com


MVP Network Consulting
Technology That Works.
Now, What?

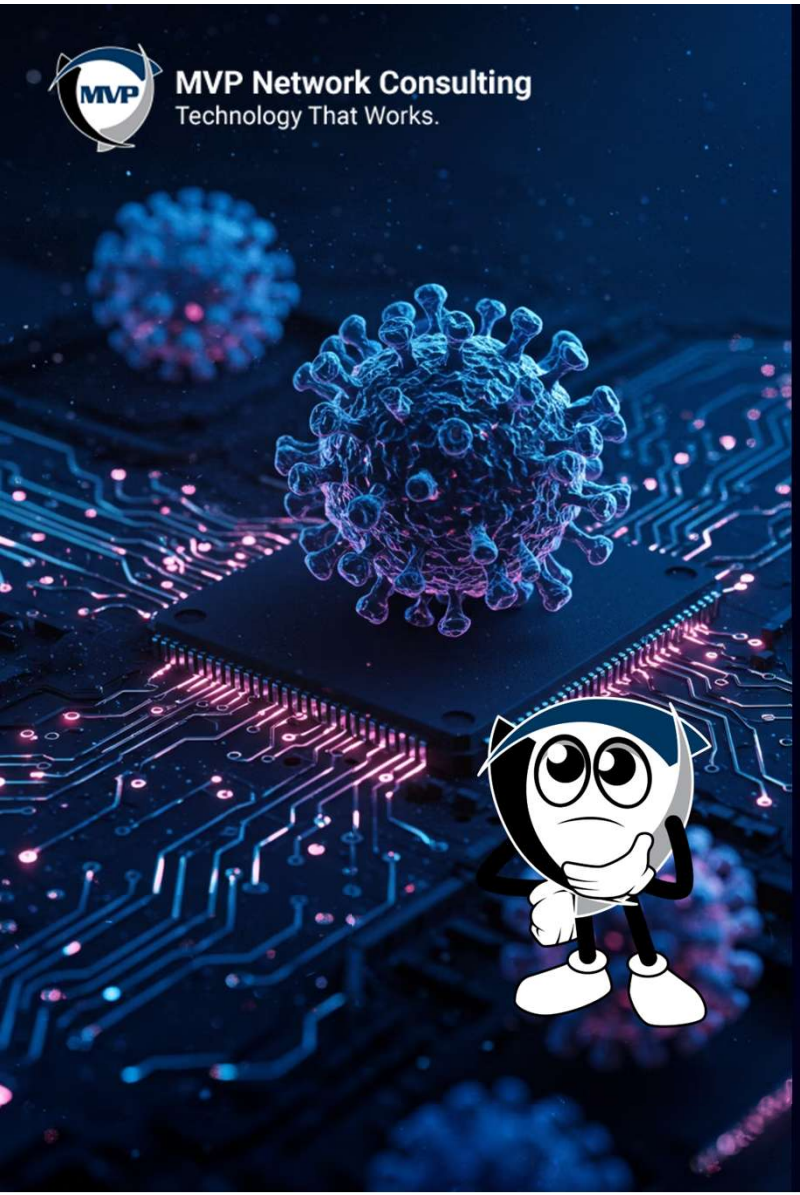

MVP Network Consulting
Technology That Works.
Recovery Starts (or Fails) Within 24 Hours
Average breach goes undetected for 204 days

The Clock Starts the Moment Chaos Hits

Most regulators give you 72 hours to report starting at hour one


MVP Network Consulting
Technology That Works.
Do you have Cyber-Insurance with a ransomware rider?

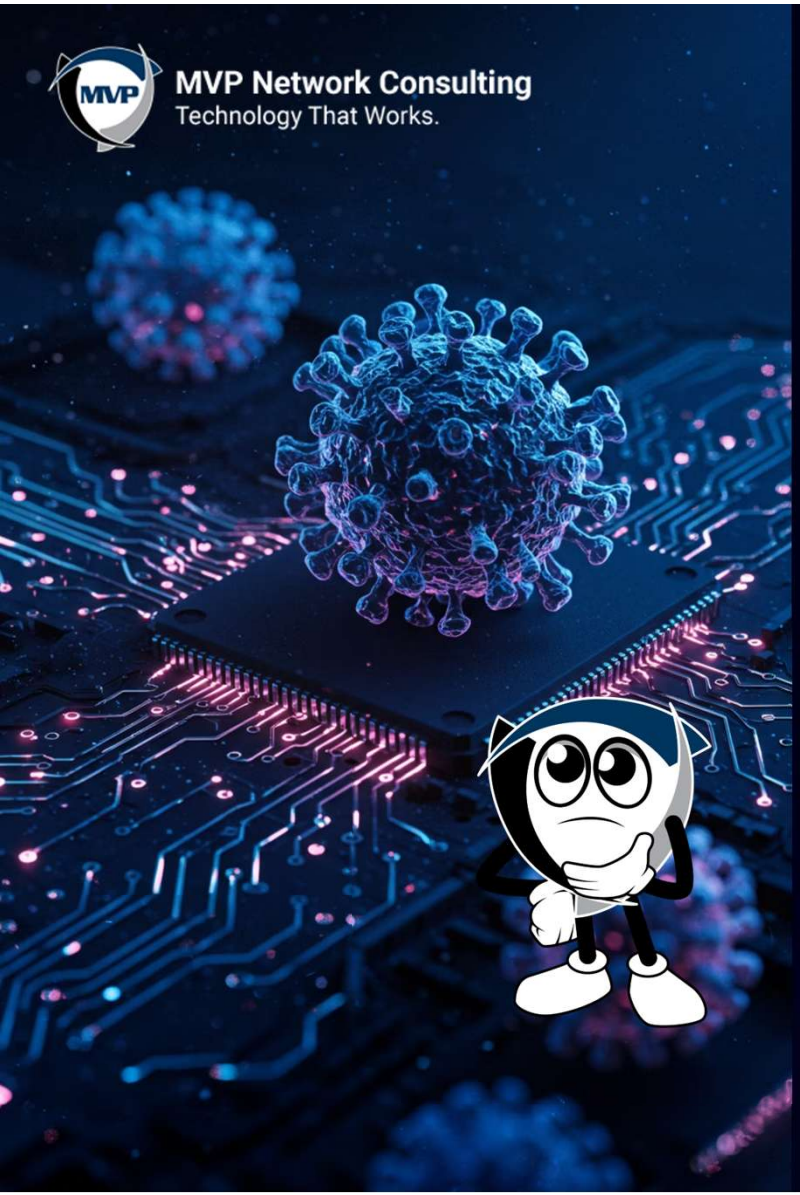

MVP Network Consulting
Technology That Works.
Do you have an existing Incident Response Plan?



Key Questions

Immediate Technical Questions

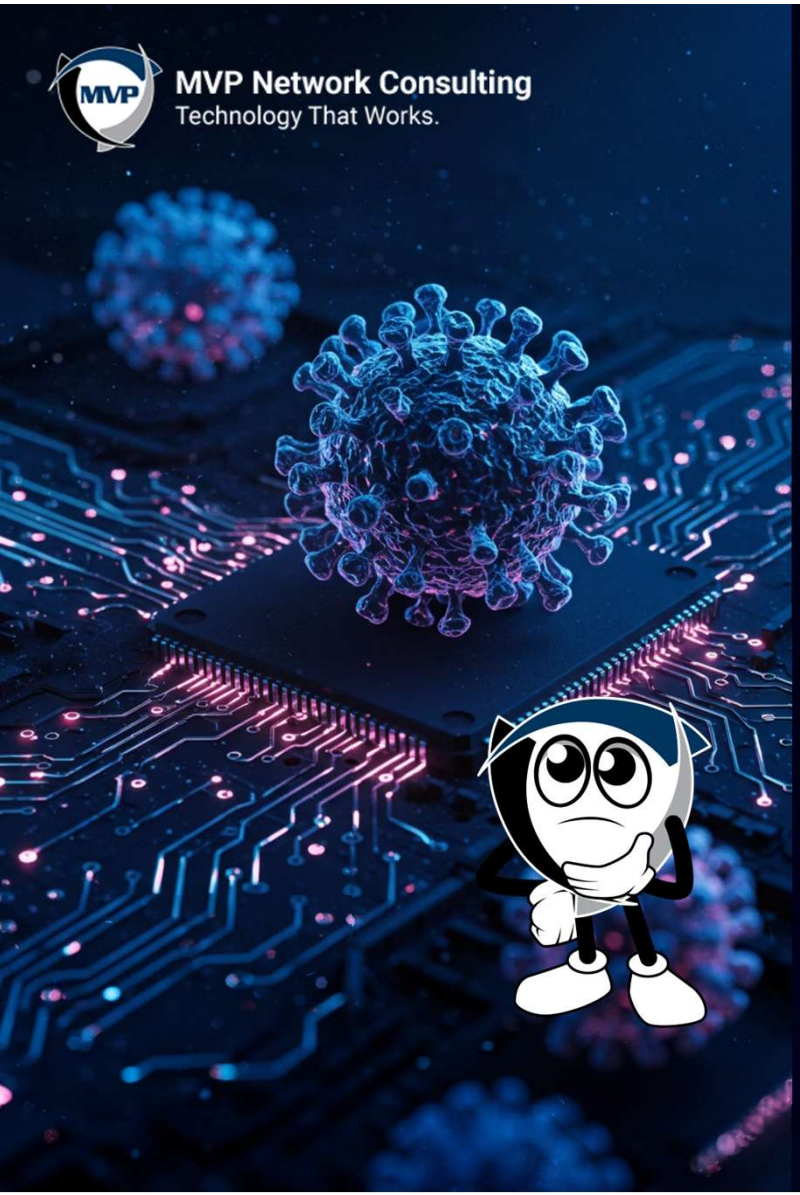
- Is the attacker still active on the network, or have they been removed?
- Which systems, servers, and endpoints are compromised or encrypted?
- Did the attacker steal data, or is it only encrypted?
- Is any personally identifiable information (PII) or regulated data affected?
- Are backups available, isolated, and uninfected?
- Has malware spread to cloud services or remote offices?
- Is there evidence of lateral movement or persistence mechanisms?
- What vulnerabilities were exploited (e.g., unpatched software, weak credentials)?
- Do we have logs, SIEM data, or forensic evidence to analyze the attack?
- Who was “patient zero”—the first compromised device or user?
- Is endpoint protection or threat hunting active and effective?
- Are our backup systems themselves targeted or compromised?
- Can we restore critical systems from clean backups, and how quickly?



Key Questions

Operational & Business Questions

- What is the scope of business impact (systems down, data loss, operational disruption)?
- Which business processes are halted, and what is the financial cost per hour of downtime?
- Who needs to be notified internally (executives, IT, legal, PR, compliance)?
- What external notifications are required (customers, partners, regulators, law enforcement)?
- Do we have cyber insurance, and does it cover ransomware?
- What are the reporting requirements (e.g., HIPAA, GDPR, SEC)?
- Is there a tested incident response plan, and is everyone clear on their roles?
- What is our communication plan for stakeholders and the media?
- Do we need to engage external experts (forensics, negotiators, legal counsel)?
- Has a ransom demand been made, and what are the risks of paying?
- What are the legal and regulatory implications of the breach?
- How do we document every action for accountability and future analysis?



Key Questions

Strategic & Recovery Questions

- How did the attack happen, and how long were attackers undetected?
- What steps have been taken to eliminate the threat and prevent recurrence?
- What lessons can be learned to strengthen future defenses?
- How do we rebuild trust with customers, partners, and regulators?
- What improvements are needed in backup, security, and staff training?
- How do we ensure resilience and continuous improvement post-incident?

MVP Network Consulting
Technology That Works.

Hour 0-1: Immediate Containment

System Isolation

Disconnect compromised servers and networks to stop malware spread and protect other systems.

Evidence Preservation

Capture volatile data like memory dumps and active connections essential for forensic analysis.

Incident Response Activation

Trigger the IR plan or assemble a response team quickly to mobilize containment and assessment efforts.

MVP Network Consulting
Technology That Works.

Communication—Who to Notify and When

- **Internal:** Notify executives, IT, legal, and PR teams immediately.
- **External:** Prepare templates for customer, partner, and regulatory notifications.
- **Media:** Have a crisis communication plan ready for public statements.
- Use secure channels for all communications during an incident

Hours 1-4: Assemble & Mobilize

Assembling the IR Team

Gather a multi-disciplinary team including IT (network and forensic), legal, PR, leadership, and external experts for effective incident response.

Secure Communication Channels

Use encrypted messaging, secure emails, and burner phones to establish protected communication during the incident response.

Forensic Triage Process

Identify patient zero, attack vector, and incident scope to guide investigation and response efforts accurately.

Hours 4-12: Investigation & Decision-Making

Log Collection and Analysis

Collect and analyze logs from endpoints, firewalls, SIEM, and DNS to trace attacker activity and identify compromised systems.

Law Enforcement Engagement

Engage agencies like FBI or CISA for support in ransomware or nation-state incidents to gain additional resources and legal aid.

Data Encryption Assessment

Manage communication with customers, partners, and regulators to maintain trust and comply with legal obligations like GDPR and HIPAA.

Hours 12-24: Stabilization & Recovery Planning

Critical System Restoration

Prioritize rebuilding essential systems like email servers, ERP, and CRM using clean images and backups.

Data Recovery Efforts

Use forensic and decryptor tools to recover data safely and efficiently after an incident.

Negotiation and Legal Approval

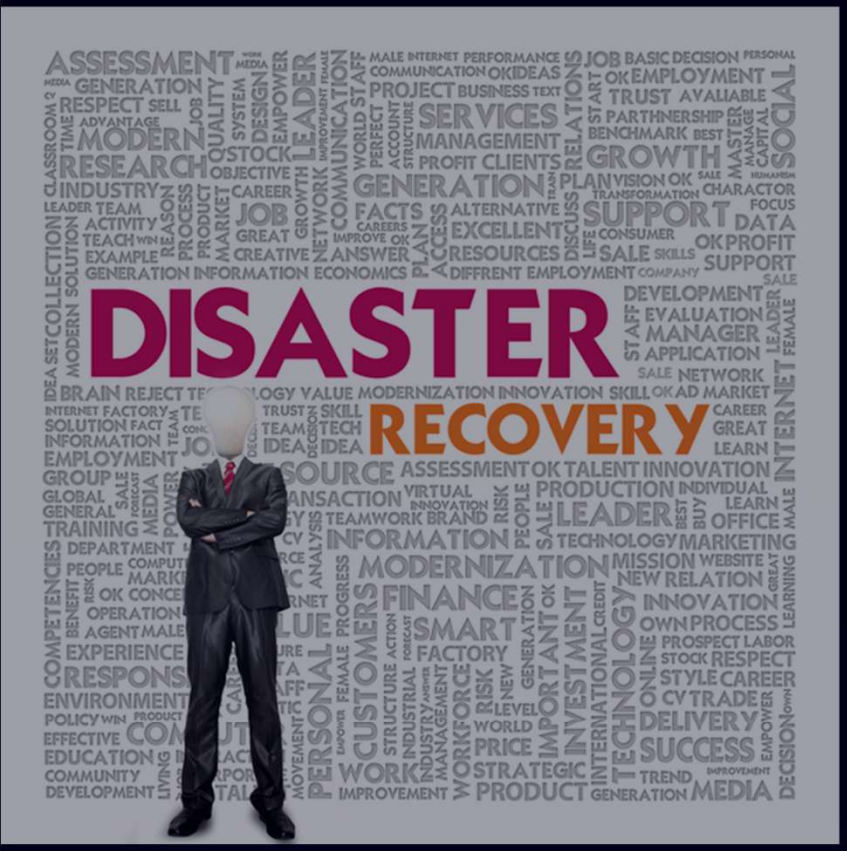
Engage expert negotiators for ransom talks with legal and executive consent considering all implications.

Documentation and Accountability

Maintain detailed timelines and records to support accountability and future incident analysis.

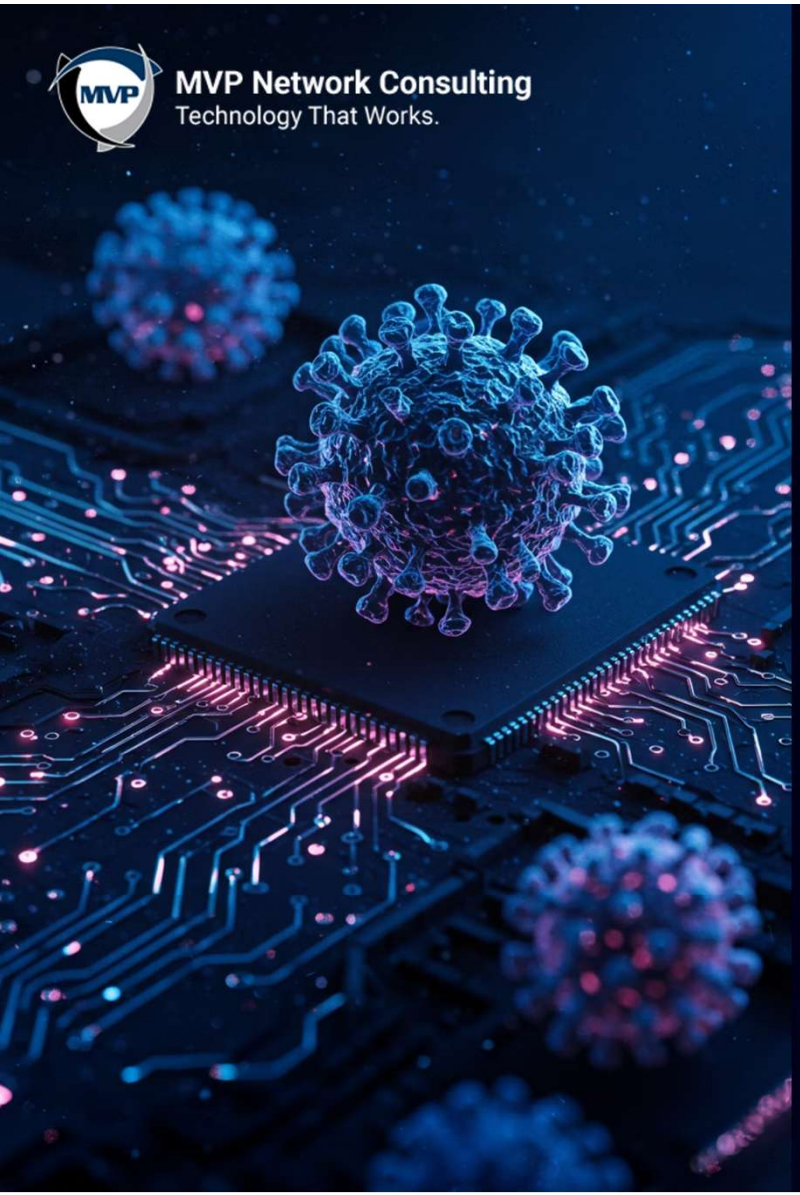
MVP Network Consulting
Technology That Works.

MVP Network Consulting
Technology That Works.



Recovery—Restoring Operations

- Prioritize restoration of critical systems (email, ERP, CRM).
- Validate backups before restoring data.
- Monitor for reinfection or persistent threats.
- Engage expert negotiators for ransom talks (if applicable).
- Document all actions for accountability.



Building Resilience Before an Attack

- Develop and regularly update an Incident Response (IR) Plan.
- Conduct tabletop exercises and simulations.
- Maintain an up-to-date asset inventory.
- Ensure backups are isolated, encrypted and tested.
- Train staff on security awareness and phishing prevention.

Resilience: Go Beyond the Crisis

Learn From It

Every disaster leaves clues.

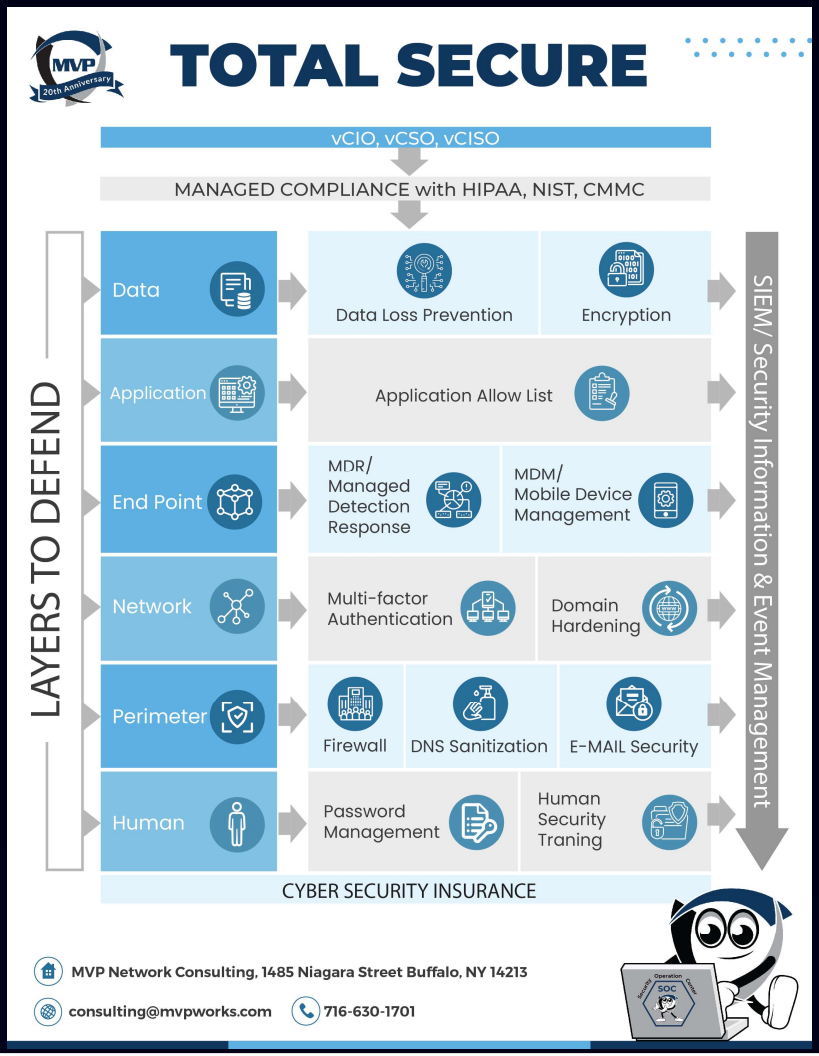
Rebuild Stronger

Don’t just recover. Reinforce.

Be Proactive

Resilience is built in the quiet hours.

How to Rebuild Stronger?




MVP Network Consulting
Technology That Works.
Consider adding a vCSO service
SCAN ME

Why You Need A Virtual Chief Security Officer vCSO

Our Virtual Chief Security Officer (vCSO) solution will help your business make security decisions, understand security threats, and optimize security processes.

With our vCSO solution, you will retain a board-level resource who can virtually sit inside your company and manage your security strategy, budget, review of risks and regulatory programs.

Get the benefit of highly-specialized security talent for a fraction of the cost of a full-time staff member

- **Threat Intelligence**
  It provides context for decisions being made within the cybersecurity program.
- **Risk Analysis**
  It prioritizes items for completion within the organization—provides a trustworthy place to start.
- **Security Accountability**
  Creates oversight for the organization's security —the Executive team knows it is being proactively managed.
- **Board-level Discussion**
  Communicate business security risk and outcomes to the board, now that it is a board-level expectation.
- **IT Meets IS**
  Someone on the team focused on making sure it gets done in a secure matter – not just done.

With Our vCSO Solution, We Will Not Be Sitting On The Sidelines

Our goal is to be constantly and consistently delivering you results.
Below we will outline the ongoing items that we will be providing as apart of this solution.

WEEKLY

IT Status Meeting (Optional)
Attend IT Status Meeting to provide updates on projects, answer tactical security questions, and get decisions from leadership as needed; review any current security vulnerabilities and discuss how the organization may or may not be impacted.

MONTHLY

IT Performance Analysis
Audit monthly IT activities, document findings and initiate/request/validate any necessary changes.

IT Security Meeting
Meeting to review issue progress, vulnerability test results, security project status, plan for upcoming events, and review/edit deliverables as needed.

Simulated phishing exercises*
Deploy simulated phishing exercises and analyze results for frequent clickers or other signs and/or anomalies (*Requires investment in advanced security stack)

Back-up Review
Review back-up of all endpoint machines and servers to ensure that they are occurring on a timely basis and are within backup service level agreement.

QUARTERLY

User Privilege Review
Review the list of Line of business, M365 and domain users to ensure no unneeded users; verify tickets were created for user termination requests as well as any Human Resources changes.

Executive Leadership Meeting
Meet with executive team (CEO, COO, CFO, GC and CAO) to provide updates on current trends in IT security, latest vulnerability analysis and status of IT projects; supplement with further updates as needed.

IT Security Training
Select and initiate IT security training to all endpoint users through the Galactic portal.

Vulnerability Scan/Security Analysis
Provide ongoing security analysis of network, provide/review report findings with leadership and assist in necessary remediation projects.

BI-ANNUALLY

Board Update Meeting
Prepare and present updates for Bi-Annual Cyber Security Risk Board Update.
Prior to update confirm content with executive team and review discussion topics.

ANNUALLY

Physical Inventory Review
Review the list of IT equipment to ensure it is up to date and all assets are accounted for.

Third-Party Penetration Testing
Schedule, coordinate and oversee third-party penetration testing; coordinate and remediate any findings from the testing.

Policy Review
Review policies and make updates based on organizational changes; if changes are made to acceptable use policy, coordinate with legal and incorporate into Employee Handbook as needed; create and implement new policies as needed.

Procedure Review
Review and update procedures

Vendor Review
Conduct security review of vendors, including completion of Vendor Self-Assessment Questionnaires; initiate/oversee vendor security changes as needed; Review most current contract to determine if updates are needed.

Risk Assessment
Review the different types of risk facing the business units; prioritize security and compliance investments and initiatives based on risk findings.

PCI Self-Assessment
Complete and save to file the annual self-assessment questionnaires for compliance purposes.

Tabletop Exercise
Perform annual table-top exercise of the disaster recovery plan/incident response plan with applicable IT vendors and company personnel.

Inventory Data Assets
Review the list of assets/vendors with the executive team on an annual basis, generally as part of quarterly IT executive meeting; review list of Key Vendors in IT security portal to ensure it is up to date.

AS-NEEDED

Site Visits: Conduct in-person visits to organization's sites to review on-site security practices and initiate necessary changes.

Threat Intelligence Emails: Provide threat intelligence emails to organization as relevant.

Audit Representation: Proper C-level representation in the event of a formal audit

Security Deliverables: Provide other security deliverables and best practices as needed.

The First 24 Hours Start Today...

SCAN ME

MVP Network Consulting
Technology That Works.

MVP Network Consulting
Technology That Works.

Here's what you can do:

Get a FREE Cybersecurity Assessment & Evaluation

mvpworks.com/cyber

SCAN ME

MVP Network Consulting
Technology That Works.

We will NOT need

Administrative Credentials

mvpworks.com/cyber

SCAN ME

MVP Network Consulting
Technology That Works.

We will NOT

Install Anything

mvpworks.com/cyber

SCAN ME

MVP Network Consulting
Technology That Works.

We Will:

Send you a link to send to 5 key users

Get you to click "run" to start the scan

Meet with you to go over the confidential report

mvpworks.com/cyber

SCAN ME

MVP Network Consulting
Technology That Works.

Questions? Contact Us Today!

Call Us

716.630.1701

Visit Us

1485 Niagara StreetBuffalo, NY 14213

Email Us

ikram@mvpworks.com