Federal Bureau of Investigation Cybercrime Executive Briefing

Courtesy of

USM Technology

Confidentiality & Intellectual Property Notice

This document, including all of its contents herein, is the proprietary and confidential property of USM Technology. It is intended solely for the use of the individual or entity to whom it is addressed.

Unauthorized distribution, dissemination, or copying of this document or the information contained within is strictly prohibited. The intellectual property, including methodologies, strategies, techniques, research, and data, is the exclusive property of USM Technology and may not be used, reproduced, or disclosed to others without the express written permission of USM Technology.

All trademarks, copyrights, patents, and other intellectual property rights referenced or contained herein are the property of their respective owners.

Any recipient of this document who is not the addressee, or who receives this document in error, should immediately notify USM Technology and destroy the document. Failure to maintain the confidentiality of this document may result in legal action against the offender.

By accessing, viewing, or using this document, you acknowledge and agree to the aforementioned terms and restrictions.

Federal Bureau of Investigation
Cybercrime Executive Briefing

Contents

Federal Bureau of Investigation Cybercrime Executive Briefing

Executive Summary

A Special Agent from the Federal Bureau of Investigation's (FBI) Dallas Cyber Task Force joined with Stephen Cracknell, CEO and Founder of USM Technology, to deliver the following cybersecurity content to a group of North Texas business leaders. The Special Agent shared details about the latest cyber-attacks happening across the United States. He also provided details on how business leaders can leverage resources available from various government agencies to harden their cybersecurity protocols and respond to a cyber-attack.

We discussed the latest tactics used by cyber criminals to pressure business leaders into making a ransom payment. After reviewing the stages of a *Human Operated Ransomware Attack,* the group conducted a mini-tabletop exercise where the realities of business leaders responding to a cyber-attack were brought to life. The event concluded with a conversation about how an organization's leadership could build a program that would enhance their ability to respond to a major cyber-attack.

Below is a digest of the content delivered during this event.

Goals

1. Familiarize participants with resources available from Federal and local government agencies.
2. Educate participants on the latest techniques and tactics used by cybercriminals.
3. Provide a framework for building strong cyber response capabilities.

Key Take Aways

- Learn how to leverage government resources both before and after an attack.
- Discover the evolving cybercrime tactics, such as double extortion, data exfiltration, and Artificial Intelligence that hackers use to enhance the effectiveness of their attacks.
- Identify cyber insurance challenges such as coverage limits, misrepresentation, evidence preservation, and recommendations on where to store your policy documents.
- Cyber Response Preparation is critical. We step through the following five vital preparation steps:
    1. Assess your defenses and critical data.
    2. Develop key policies and procedures.
    3. Gather critical documentation.
    4. Build your response team.
    5. Have a safe place to meet and collaborate.

Government Resources

Homeland Security CISA (Cybersecurity and Infrastructure Security Agency) - https://www.cisa.gov

Primary Role: CISA is the nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

Activities:

- Provides cybersecurity tools, incident response services, and assessment capabilities to safeguard the .gov networks.
- Shares critical information and offers training and resources to government and private sector partners.
- Issues advisories and alerts on cyber threats.

Treasury Department- https://home.treasury.gov

Primary Role: The Treasury Department oversees the financial infrastructure of the country and has a role in protecting financial systems from cyber threats.

Activities:

- Monitors financial transactions to detect and deter illicit activities such as money laundering, which can be linked to cybercrimes.
- Collaborates with other federal agencies and private sector entities to improve the cybersecurity framework of financial institutions.
- Can impose financial sanctions on malicious cyber actors and entities.

Federal Bureau of Investigation **(FBI)**- https://www.fbi.gov & https://www.ic3.gov

Primary Role: The FBI is the primary federal agency for investigating cyber-attacks & intrusions.

Activities:

- Investigates and combats cybercrimes including hacking, ransomware, identity theft, and cyber espionage.
- Shares intelligence and threat information with public and private sector entities.
- Offers cybercrime victim support and engages in public outreach and education on cyber threats.

Local Authorities: Varies

Primary Role: They address cyber incidents and crimes at the local and regional level, offering first-response and coordination with higher authorities.

Activities:

- Investigate local cyber incidents & crimes, such as frauds and scams affecting businesses.
- Act as a liaison between local entities and larger federal bodies in response to significant cyber incidents.
- Engage in community outreach and education on cyber threats and best practices.

Federal Bureau of Investigation
Cybercrime Executive Briefing

Cybercriminal Techniques & Tactics

Cybercriminal Tactics

Cybercrime is any illegal activity that involves the use of a computer or a network to harm individuals, organizations, and governments by affecting their security, privacy, finances, reputation, and operations.

Popular Techniques for Inflicting Damage

Social Engineering – The impersonation of a trusted person or entity to request money, information, or access from the target.

Data Exfiltration- The theft or unauthorized removal or movement of any data from a network later used to extort an organization’s leadership or is sold to unauthorized entities.

Ransomware – The use of malicious software to encrypt the victim’s data or device and demand a ransom for its decryption or release.

Cloud Security Vulnerabilities- Weaknesses or flaws in the design, implementation, or operation of cloud services or systems that can be exploited to compromise the security, privacy, or functionality of the cloud or its users.

Supply Chain Attack – Hackers target the weakest link in a chain of trust. If one organization has strong cybersecurity but an insecure trusted vendor, the attackers will target that vendor. With a foothold in the vendor’s network, the attackers can then pivot to the more secure network using that trusted relationship.

5 Ways Hackers Pressure Executives To Pay The Ransom

1. Personalized Threats: Hackers may gather information about key executives or employees and use it to personalize threats. They might send targeted messages that include personal details or threats against the safety of individuals, creating immense pressure on leaders to pay the ransom.
2. Countdown Clock: To create urgency, hackers set a timer, warning that the ransom will increase, or critical data will be permanently deleted unless payment is made swiftly. The impending deadline pressures executives into making quick decisions to avoid higher costs or data loss.
3. Fake Legal Threats or Impersonation of Authorities: Cybercriminals masquerade as law enforcement agencies or legal entities, claiming regulatory violations or legal actions against the organization. Fearing legal and regulatory consequences, executives may opt to pay the ransom.
4. Threaten to Inform Media, Employees, or Clients: Hackers threaten to publicize the breach, potentially damaging the organization's reputation. The fear of adverse publicity, loss of employee trust, or client confidence can coerce executives into paying to keep the breach under wraps.
5. Destruction of Backup Data: To eliminate recovery options, hackers may target and destroy backup copies of the encrypted data. This leaves the victim organization with limited options for restoring their systems and data, increasing the likelihood that they will pay the ransom as a last resort.

How Much Could A Major Cyber Crime Incident Cost A Midsize Organization?

Breakdown of costs for a 150-employee business to recover from a major cyber-attack.

The cost of recovering from a major cyber-attack for a 150-employee business can vary depending on the extent of the attack and the specific aspects of the industry. However, here is a general breakdown of potential costs to help you understand the financial implications of such an event:

1. Incident response and investigation:
   - Hiring external cybersecurity experts: $20,000- $50,000
   - Internal team costs: $10,000- $30,000
   - Forensic investigation: $25,000- $75,000

2. Remediation and recovery:
   - System and network repair or replacement: $50,000- $150,000
   - Data restoration and recovery: $25,000- $100,000
   - Software and hardware upgrades: $20,000- $75,000
   - Employee training and awareness programs: $10,000- $30,000

3. Legal and regulatory costs:
   - Legal counsel and fees: $25,000- $100,000
   - Regulatory fines and penalties (HIPAA, HITECH, GDPR, etc.): $50,000- $500,000 (could be even higher, depending on the severity of the breach)
   - Compliance audits and assessments: $10,000- $40,000

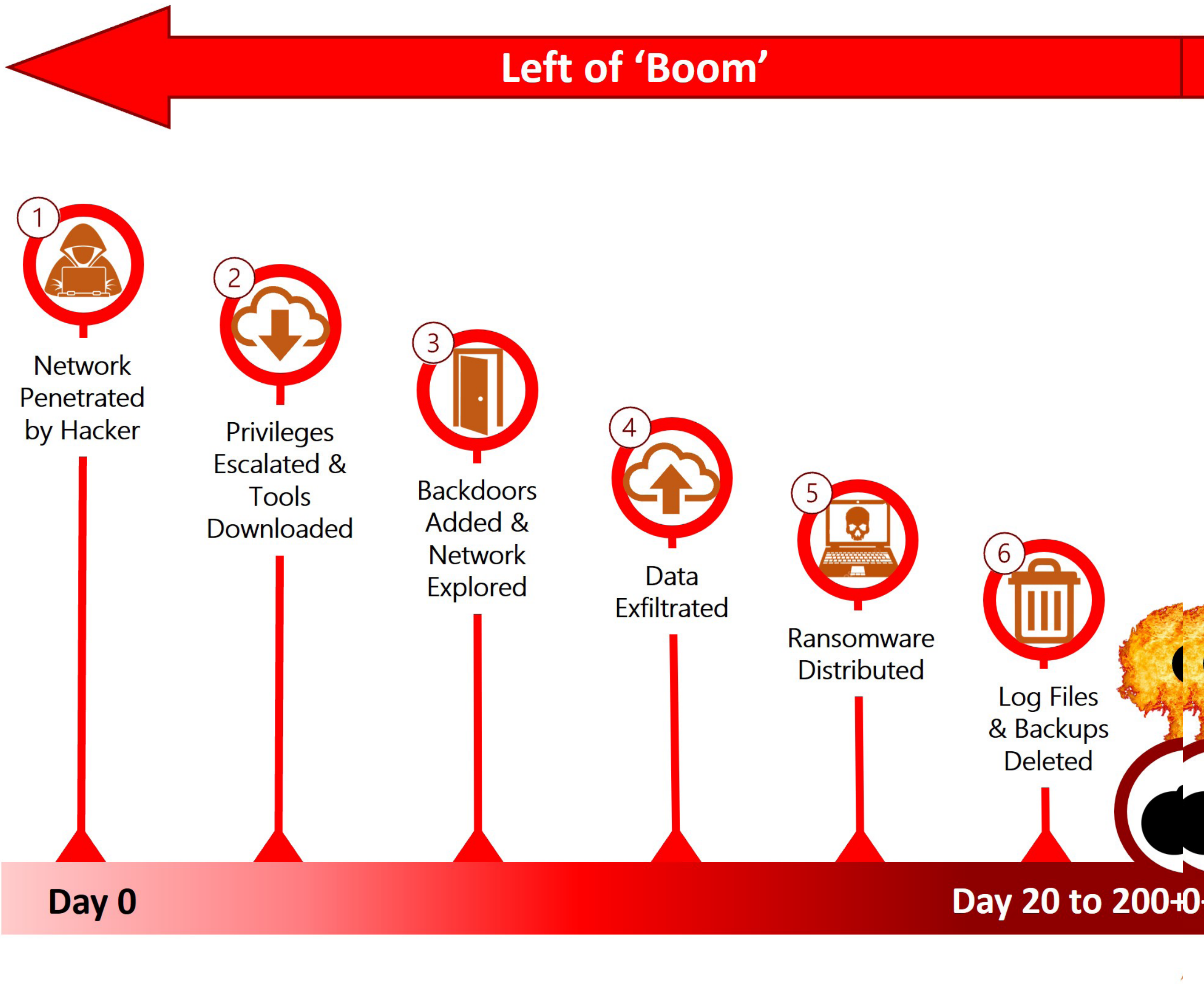
4. Public relations and communications:
   - Crisis communication and PR management: $10,000- $50,000
   - Notification to affected patients and stakeholders: $5,000- $20,000

5. Business interruption and lost revenue:
   - Downtime and productivity loss: $100,000- $500,000
   - Loss of client trust and potential customer churn: $50,000- $250,000

6. Cyber insurance and risk management:
   - Cyber insurance premiums: $15,000- $50,000 (annually)
   - Risk management and mitigation planning: $10,000- $30,000

These cost ranges are rough estimates, and the actual costs may vary based on factors such as the size of the breach, the specific systems and data affected, and the business's existing cybersecurity measures. The total recovery costs for a 150-employee business could range from ***$300,000 to over $1.5 million, not including*** potential ongoing expenses related to ***reputational damage*** or ***legal liabilities***.

Human Operated



Left of 'Boom'

1 Network Penetrated by Hacker

2 Privileges Escalated & Tools Downloaded

3 Backdoors Added & Network Explored

4 Data Exfiltrated

5 Ransomware Distributed

6 Log Files & Backups Deleted

Day 0

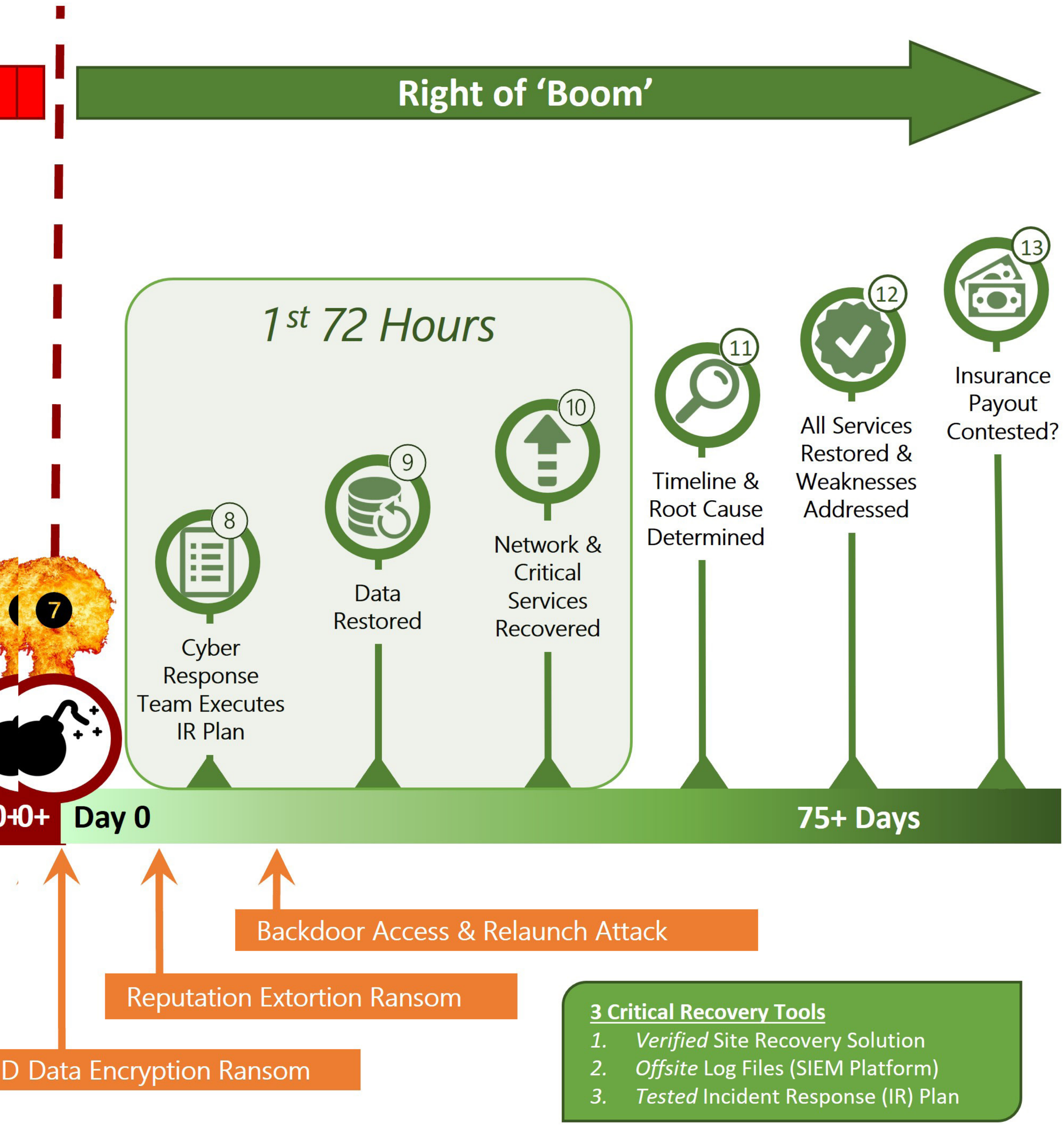
Day 20 to 200+

3 Most Common Attack Vectors

1. Phishing / Social Engineering
2. Unpatched Systems
3. Compromised Credentials

D D

Ransomware Attack


Right of 'Boom'
1st 72 Hours
7
8
Cyber Response Team Executes IR Plan
9
Data Restored
10
Network & Critical Services Recovered
11
Timeline & Root Cause Determined
12
All Services Restored & Weaknesses Addressed
13
Insurance Payout Contested?
0+
Day 0
75+ Days
Backdoor Access & Relaunch Attack
Reputation Extortion Ransom
D Data Encryption Ransom

3 Critical Recovery Tools

1. *Verified* Site Recovery Solution
2. *Offsite* Log Files (SIEM Platform)
3. *Tested* Incident Response (IR) Plan

Tabletop Exercise Explained

Cybersecurity tabletop exercises are not mere simulations; they are strategic investments in your organization's cyber resilience. They foster collaboration, reveal vulnerabilities, and empower us to make informed decisions in times of crisis. In an era where cyber threats are ever evolving, these exercises are an essential tool to safeguard your organization’s data, operations, and reputation.

What is a Tabletop Exercise?

A tabletop exercise is a dynamic and collaborative simulation of a cyber incident. Typically lasting 2 to 4 hours, it brings together a team of people to evaluate your organization’s response capabilities:

1. **Facilitator:** Guides the exercise, sets the scenario, and ensures smooth progression.
2. **Participants:** Key stakeholders from various departments who actively engage in the simulation.
3. **Observers & Evaluator:** Individuals who assess and evaluate the participants' responses.
4. **Scribe / Timekeeper:** Maintains records and manages time during the exercise.

Recommended Agenda:

1. **Introduction:** Setting the stage for the exercise, emphasizing open communication, and promoting a no-fault environment.
2. **The 'Incident':** Presenting a realistic cyber threat scenario that challenges participants to respond as if it were a genuine crisis.
3. **Questions & Open Dialogue:** Encouraging discussion, decision-making, and coordination among participants.
4. **Hotwash and Evaluation:** Reflecting on the exercise's outcomes, identifying strengths, and pinpointing areas for improvement.
5. **Next Steps Discussion:** Formulating an action plan based on lessons learned and exploring strategies for refining our cybersecurity posture.

Benefits:

Cybersecurity tabletop exercises serve as a crucible for enhancing your resilience against cyber threats by:

1. **Testing Response Effectiveness:** It examines your organization's ability to respond adeptly during a significant cyber incident. This includes evaluating your capacity to coordinate information sharing, manage communications with stakeholders, such as investors, clients, employees, and law enforcement, and even simulate interactions with potential adversaries, like hackers.

2. **Identifying Improvement Areas:** By exploring various aspects of incident response, these exercises uncover weaknesses and deficiencies in your cyber incident response plans, enabling you to refine and enhance your strategies.

3. **Resource Management:** In a realistic scenario where internal resources may be exhausted, the exercises help you effectively explore processes for requesting and deploying additional response resources.

Mini Tabletop Exercise

Friday Afternoon at 4 p.m.- Thanksgiving Weekend

You receive a call from your controller, they say they can no longer log onto their work computer through the firewall. You ask your IT team to investigate, and they alert you that they ***can no longer log into the firewall***. After a visit to the office, your IT team reports that many of your organization's computers display a blank red screen. A ***ransom message*** has appeared on some of your computers demanding $230,000 worth of Bitcoin for the decryption key and a warning that the cost will double unless payment is received within the next 48 hours.

Later that evening, your IT team receives an email from a security researcher. The researcher reports that they discovered a series of posts from a well-known cybercrime syndicate on the Dark Web. The researcher believes the posts are genuine. The posts contain obvious indicators that the threat actors have gained access to personally identifiable information (PII), including ***employee*** social security numbers, cell phone numbers, and home addresses. They also have ***customer*** contact details, bank accounts, and routing numbers. The hacker group has provided a small number of data records to validate their claims, and according to the posts, they are willing to sell the information for “the right price.”

The Initial Assumptions

The hackers have:

- Taken control of your network.
- Breached your cloud-based HR and ERP systems and exfiltrated sensitive data.
- Infected an unknown number of employee workstations with ransomware.

Tabletop Questions

1) Where does your leadership team meet to gather data and plan your response?
2) Which outside parties would you involve at this stage, and who would you call first?
3) What are your organization’s priorities at this point?
4) What are the technology dependencies on your mission-critical business functions, for example, payroll, AR/AP, operations, and sales?
5) What other ways could the hackers ‘increase the pain’ at this stage?
6) What will your message be to employees, clients, and investors?
7) If the media calls and asks for a comment, who will respond, and what will they say?

Federal Bureau of Investigation
Cybercrime Executive Briefing

Building Effective Cyber Response Capabilities

Cyber Insurance Considerations

- Ensure the overall coverage limits (and 'sub-limits') are sufficient to pay for downtime & recovery.
- Be aware that social engineering & business email compromise sub-limits can be notably lower.
- Beware of "Misrepresentation"- Carriers can deny a claim if you attested in the insurance application that a security control was in-place but that control was not active during an attack.
- Have your legal team and/or insurance broker review the fine print.
- Keep your insurance policy "off-network". Hackers are searching for it after they breach your network and will use knowledge of your coverage limits during the 'negotiation' phase.
- The carriers will want to gather evidence after an attack. Be sure to work closely with them during the recovery phase.

Core Cybersecurity Best Practices

- Update systems regularly
- Enforce Two Factor Authentication
- Conduct Phishing tests and training for employees
- Maintaining offline backups
- Having a tested Incident Response Plan
- Have an "out-of-band" communication method for key employees

Cyber Response Preparations

1. Assess Your Defenses and Critical Data
2. Prepare Your Response Team
3. Gather Your Documentation
4. Create and Organize Your Secure Meeting Space
5. Conduct a Tabletop Exercise

Critical Data

1. Lists of Assets and User
2. 3rd Parties: Vendors, Clients, Investors
3. Network Topology
4. Configuration Data
5. Vulnerabilities (Pen Test, Patch Status)
6. Log Information (Sent to SIEM)

Speed Dial: Your Cyber Recovery Team Members

In-House Team

1. Leadership
2. Technology
3. Business Units

Technical Team

1. Forensics
2. Cyber Response
3. Cyber Recovery

Business Team

1. Legal
2. Cyber Insurance
3. Public Relations
4. Law Enforcement

Critical Cyber Response Policies & Procedures

1. Business Continuity Plan
2. Risk Assessment
3. Business Impact Analysis
4. Incident Response Plan
5. Disaster Recovery Plan

The Process:

1. **Analyze Your Network and Assets:** The first step is to understand what you're protecting. Identify your network's critical assets, data, and systems. This forms the foundation of your response program.

2. **Document Your Resources and Construct Plans:** Document everything you've identified in step one. Develop clear response plans, policies, and procedures tailored to your organization's unique needs. This documentation ensures that everyone knows what to do during a cyber incident.

3. **Build Your Response Team:** Assemble a response team consisting of skilled individuals from various departments. Define their roles and responsibilities within the response program. Effective communication and collaboration are key.

4. **Build a Secure Environment for Crisis Communications:** Establish a secure communication channel for your response team. Ensure critical recovery data is housed in a protected environment, shielding it from potential cyber threats.

5. **Test and Validate Your Plan:** Regularly test your response plans through tabletop exercises and simulated incidents. Validate your team's readiness and identify areas for improvement. A well-tested plan is a resilient plan.

Deliverables and Output:

Your Post-Attack Cyber Response program will comprise:

1. **Response Plans (Policies & Procedures):** These documents serve as your playbook during a cyber incident. They provide step-by-step guidance on how to respond, minimizing confusion and ensuring a swift response.

2. **Critical Data:** Your program includes a repository of critical data, encompassing team member information, key employee contacts, client details, network configurations, and asset inventories. This information is crucial for informed decision-making during a crisis.

3. **Secure Housing:** To protect your response plans, critical recovery data, and secure communications, a secure environment is established, safeguarding your most valuable assets from cyber threats.

In conclusion, building a Post-Attack Cyber Response program is a proactive step in safeguarding your business from cyber threats. It is a process that involves careful analysis, documentation, team building, and rigorous testing. The deliverables provide a solid foundation for an effective response to a cyber incident, helping you mitigate damage and reduce downtime.

The team at USM is committed to ensuring your cybersecurity resilience. If you want help developing your organization's cyber-attack survival system, please request an initial meeting with Stephen at: https://bit.ly/usm-quickchat.

Appendix

Glossary of Technical Terms That Every Business Leader Should Know

1. **MFA (Multi-Factor Authentication):** An authentication method requiring multiple verification factors.
2. **APT (Advanced Persistent Threat):** A prolonged and targeted cyber-attack where the attacker remains undetected.
3. **SIEM (Security Information and Event Management):** The real-time analysis of logs and security alerts.
4. **SOC (Security Operations Center):** A facility where cybersecurity professionals monitor, manage, and respond to security incidents.
5. **External Vulnerability Scan:** A process used to identify, classify, and prioritize the vulnerabilities of an organization's external-facing assets.
6. **Penetration Testing (Pen Test):** An authorized cyber-attack on a computer system performed to evaluate the system's security.
7. **Risk Assessment:** An evaluation to identify, quantify, and prioritize organizational risks.
8. **Business Continuity Plan (BCP):** A plan ensuring business processes can continue during a major disruption or disaster.
9. **Disaster Recovery Plan (DRP):** A documented process to recover and protect a business IT infrastructure during a disaster.
10. **Business Impact Analysis (BIA):** An analysis that predicts the consequences of a disruption to critical business processes and the documentation of dependencies.
11. **Incident Response Plan**: a documented set of actions to respond to a cybersecurity incident. An incident is any event that compromises data confidentiality, integrity, or availability.
12. **Forensics Team:** Specialists who investigate and analyze details of cyber incidents to provide evidence and insights.
13. **Cyber *Response* Team:** A group responsible for responding to cyber incidents, ensuring they're managed effectively.
14. **Cyber *Recovery* Team:** Specialists focused on restoring systems and data after a cyber incident.
15. **RPO (Recovery Point Objective):** Denotes how much data an organization can afford to lose after a cybersecurity incident.
16. **RTO (Recovery Time Objective):** Represents how quickly a business needs to recover operations after a breach.
17. **IAM (Identity and Access Management):** A framework to ensure authorized access to resources.
18. **DLP (Data Loss Prevention):** Technologies and policies that prevent unauthorized access to or loss of sensitive data.

6 Cyber Myths

1. **My business is too small to be targeted.**
   Small businesses are often targeted because they tend to have weaker security measures. Hackers can use bots and scripts to automate many of the steps needed to breach a network then run those tools on tens of thousands of small and mid-sized businesses simultaneously.

2. **Cybersecurity is solely the IT department's responsibility.**
   Everyone in an organization should be trained, and the entire leadership should have a plan in place to effectively respond to the business implications of a major cyber-attack.

3. **A firewall, anti-virus and 2FA is enough to keep my network safe.**
   While these tools are essential, they are only part of a comprehensive security approach. Hackers have developed methods to circumvent all these controls.

4. **Once my data is in the cloud, it's the provider's responsibility to secure it.**
   While cloud providers have security measures, it's also your responsibility to ensure data access controls, and security protocols are in place.

5. **Security breaches are always immediately noticeable.**
   Many breaches go undetected for long periods. Regular monitoring and audits are crucial.

6. **More cybersecurity tools mean better protection.**
   Having too many tools can complicate security management. Robust cybersecurity is about having the right tools, policies, and staff training.

Federal Bureau of Investigation
Cybercrime Executive Briefing

Cybersecurity Quotes

“I changed all my passwords to ‘incorrect’. So, whenever I forget, it will tell me, 'Your password is incorrect'.”
— Unknown

“Someone cracked my password. Now I need to rename my puppy.”
–Unknown

"You aren't too small to be hacked, just too small to make the news."
— Zachary Kitchen

“It takes 20 years to build a reputation and a few minutes of a cyber-incident to ruin it.”
— Stephane Nappo

“A breach alone is not a disaster, but mishandling it is.”
— Serene Davis

Interesting Cybercrime Facts

1. **Phishing**: Phishing attacks are responsible for more than **80%** of reported security incidents. *Source: CISCO Cybersecurity Threat Trends Report*
2. **Costly Data Breaches**: The global average data breach cost in 2023 was USD $4.45 million, a 15% increase over 3 years. *Source: Cost of a Data Breach Report by IBM and the Ponemon Institute.*
3. **Long Detection Time**: On average, it takes companies about **280 days** to detect and respond to a cyber-attack. *Source: Cost of a Data Breach Report by IBM and the Ponemon Institute.*
4. **Artificial Intelligence (AI) in Cybersecurity**: By 2025, AI is expected to become a core component of cybersecurity strategies, not just for defense but also because malicious actors will employ AI to craft attacks. *Source: Forrester*
5. **Supply Chain Attacks**: Cybercriminals are increasingly targeting supply chains. The 2020 SolarWinds hack impacted thousands of companies and governmental agencies, spotlighting how attackers can exploit a single vulnerability in a widely used software to compromise many entities. *Sources: The New York Times, BBC, and Reuters*
6. **Funding North Korea’s Weapons Research:** 50% of North Korea’s research budget for rocket development is sourced from cybercrime payouts. *Source: The Wall Street Journal*

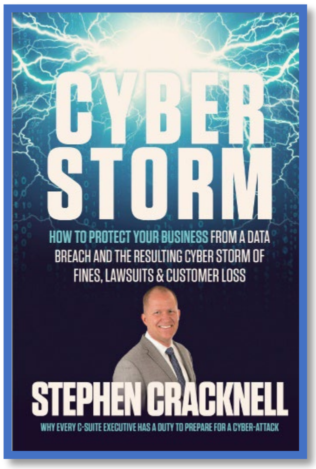
About Stephen Cracknell

Stephen Cracknell is the Founder & CEO of USM Technology and Best-Selling Author of Cyber Storm. Stephen is passionate about helping his clients use their technology to gain a competitive advantage. He set up his Texas-based company in 2010. USM Technology provides a wide range of IT services, including cybersecurity solutions, cloud and network infrastructure, and Microsoft 365 expertise. The team at USM also helps their clients with complex IT projects ranging from compliance, to cost management to mergers & acquisitions.

Before launching USM, Stephen spent 12 years at Microsoft. During his tenure at Microsoft Stephen managed a wide range of technology projects, from cybersecurity to database and network design. In 2007, Bill Gates himself awarded Stephen the Microsoft Innovation Award for his work on a Shelter Registration System he designed for the American Red Cross.

Stephen has also dedicated time to Voices for Innovation, a group that engages politicians to promote STEM education and drive forward legislation on technology privacy, and security. And when it comes to cyber- safety, Stephen's on the frontline as a cybersecurity expert for the CyberPeace Institute. The CyberPeace Institute helps protect vulnerable NGOs around the world from cybercriminals.

MSP SUCCESS
From Cybersecurity To Productivity: How
Stephen Cracknell
Of USM Technology Is Innovating To Protect And Transform Businesses
Page 14
Magic Johnson
12 "Magic" Strategies Used To Go From Basketball Star To Billionaire Businessman
Page 18
18 Laws Of Success From Shark Tank's Robert Herjavec
Page 10
MSP SUCCESS
Special Edition
MSPSuccess.com
Stephen Cracknell, CEO & Co-Founder, USM Technology


CYBER STORM
HOW TO PROTECT YOUR BUSINESS FROM A DATA BREACH AND THE RESULTING CYBER STORM OF FINES, LAWSUITS & CUSTOMER LOSS
STEPHEN CRACKNELL
WHY EVERY C-SUITE EXECUTIVE HAS A DUTY TO PREPARE FOR A CYBER-ATTACK

Buy Cyber Storm
https://bit.ly/cyber-storm

Request A Meeting
https://bit.ly/usm-quickchat

About USM Technology

USM Technology

At USM Technology, we offer a range of solutions to enhance your business's cybersecurity posture:

Cybersecurity Services

- Develop a robust *First 72 Hour Cyber-Attack Survival System*.
- Conduct *Penetration Tests* to identify vulnerabilities that hackers may exploit.
- Perform *Vulnerability Scans* to uncover open ports and address unpatched firewalls.
- Deliver *Cyber Recovery Services* to aid your organization in the aftermath of a cyberattack.
- Access a comprehensive *Cybersecurity Suite*, equipping you with the necessary tools to secure cost-effective cyber insurance and safeguard your organization.

Additionally, we provide the following technology services:

- Managed and Co-Managed IT Services
- Cloud and Network Infrastructure
- Microsoft 365 Optimization
- Flexible IT Consulting Services

The team at USM Technology is dedicated to helping you bolster your cybersecurity defenses and optimize your IT infrastructure, ensuring your business remains resilient in the face of evolving cyber threats.

You will find more information and resources on our website at https://usmtechnology.com

If you want to discuss your organization's cybersecurity strategy, you can request a meeting with Stephen here.

https://bit.ly/usm-quickchat