SERVICE SHEET

Cybersecurity Ransomware Prevention

An intelligence-led, expert-driven, strategic approach to global cybersecurity challenges affecting your organization – your people, your operations, and your reputation.

Ransomware attacks are on the rise with over 4,000 reported each day. These attacks disrupt business, cause financial and reputational harm, and even affect customers' lives. A strong focus on preventative measures can help ensure your business is ready to defend against and quickly recover from ransomware. FTI Cybersecurity can help mitigate the threat of ransomware through regular gap assessments and other readiness services.

Although only a fraction of ransomware intrusions are reported, cyber criminals ask for $5,000 to upwards of $25 million in payments. Regardless of the dollar value of the requested ransom, the financial, regulatory, and reputational costs from recovery efforts due to inadequate security protections can often far exceed the ransom. In 2021, double-extortion is exceedingly becoming a part of ransomware attacks where even paying the ransom may not be enough to move on from an attack. Effective upfront planning will thwart many ransomware attacks and allow you to recover quickly if you are impacted.

Important Questions You Should be Asking

- Are your security controls tailored to the threat of ransomware?
- Does your staff know what to do if their workstations are disabled in a ransomware attack?
- When did you last test your response capabilities to a ransomware attack?
- When did you last test your ability to restore systems from offline backups?

Ransomware Checklist

1. Conduct cybersecurity risk analysis to determine vulnerabilities.

2. Identify what and where your critical data is and ensure it is properly protected.

3. Keep operating systems, software, and applications current and patched, and set sure anti-virus and anti-malware solutions to automatically update.

4. Perform penetration testing to assess the security of your systems and ability to defend against an attack.

5. Back up and secure data regularly. Make sure they are not connected to the computers they are backing up.

6. Use standard user accounts versus accounts with administrative privileges whenever possible.

7. Utilize multi-factor authentication and configure operating systems to allow only authorized apps.

8. Restrict personally owned devices on work networks and avoid using personal apps on work computers.

9. Assess protected information (i.e. PII) and environments (IT v. OT) for vulnerabilities and proper segmentation.

10. Train staff on cybersecurity best practices. Think before clicking on a link or downloading an attachment.

How FTI Cybersecurity Can Help

FTI Cybersecurity experts have industry-proven experience preparing for ransomware and offer a multitude of services to help organizations of all scopes and sizes prepare for security incidents and especially ransomware attacks. In addition to assessing your readiness, our experts will work with you to close security gaps in a timely and resource-effective manner.

Gap Assessments

A gap assessment of your organization's cybersecurity policies, procedures, and controls is crucial for preparing to defend against ransomware incidents and ensuring business continuity. Our experts will identify where security measures are implemented, where they need to be improved, and where coverage is missing. Understanding that resources are often limited, our experts provide risk-based prioritization of remediation efforts and actionable recommendations that align the information security program with industry standards.

Business Continuity Plan Assessment

Business Continuity Planning (BCP) involves a comprehensive process of threat identification, business impact analysis, and asset classification. From there, a resiliency framework can be established that defines response protocols. Once the BCP assessment is implemented, it should be tested and altered. We are well-situated to shepherd organizations through the BCP process, whether you are starting from scratch or are evaluating existing business continuity plans.

Vulnerability Assessments

Vulnerability assessments are critical to an organization's reputation and bottom-line operations. Our experts design custom vulnerability assessment plans to ensure your infrastructure is secure and stable, preventing cyber actors from infiltrating systems. Regular assessments allow our team to test systems for any irregularities, inconsistencies, and anomalies that might render an organization's network vulnerable to ransomware.

Incident Response Plan Assessment

Your Incident Response Plan (IRP) should define the processes and procedures followed in the event of a ransomware attack, from triaging the incident based on possible impact, through getting impacted systems back online. We review the IRP with a focus on ensuring the document is suited to the organization's individual needs and priorities. We can provide recommendations to guide the client's IT staff in detecting, responding to, and recovering from a ransomware attack.

Data Mapping

Our experts provide a hybrid and all-encompassing approach to data mapping that expands beyond traditional privacy and compliance by diving deep into your organization's enterprise asset footprint. We hunt and document internal system architecture, product infrastructure, and personal data flow to provide full transparency into your systems to reduce risk. This approach ensures that your sensitive data does not fall into the wrong hands.

Additional Readiness Services

Building a robust security posture is the best way to prevent a breach from occurring. You cannot control if you will be the victim of a cyber attack or not, but you can control how to respond to one. Effective and tailored incident prevention measures can help preserve your corporate reputation, operations, and financial standing. Waiting until an incident has occurred to act is too late. Additional readiness services include:

- Perimeter Defense Analysis
- Backup & Recovery Architecture
- Organizational Material Review
- Penetration Testing and Red Teaming
- Crisis Simulations & Table-top Exercises
- Threat-Hunting Operations
- Security Awareness and Training exercises

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

No other firm in the space has a crisis communications practice

Integration of FTI Consulting's expertise across the platform

1982

Year Founded and $4.8BLN equity market capitalization*

8/10

Advisor to 8 of the world's Top 10 bank holding companies

6,400+

Employees

NYSE:FCN

Publicly traded

96/100

Advisor to 96 of the world's top 100 law firms

55

55 of Fortune Global 100 corporations are clients

**Number of total shares outstanding as of April 22, 2021, times the closing share price as of April 29, 2021.*

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

KYUNG KIM
Head of Cybersecurity, APAC
Senior Managing Director
+82 2 2190 3727
kyung.kim@fticonsulting.com

DAVE HARVEY
Managing Director, EMEIA
London
+44 207 632 5147
dave.harvey@fticonsulting.com

KEVIN WONG
Managing Director, EMEIA
Dubai
+971 54 586 7142
kevin.wong@fticonsulting.com