DealersEdge®

SPECIAL REPORT

Navigating the Aftermath: Strategies to Mitigate Future Disasters Post-CDK

July, 2024

Table of Contents & Topic Abstracts:

In the wake of the recent CDK data breach cybercrime has once again been thrust to center stage with an estimated $600 million to $1 billion in lost revenue due to dealership operations being halted for weeks.

While immediate solutions to protect dealer data are necessary, it's crucial to think about long-term strategies to recover and prepare for future unexpected events.

This DealersEdge Summary Report focused on a detailed discussion by Erik Nachbahr, Founder and President of Helion Technologies and a Certified Information Systems Security Professional (CISSP) about cybersecurity threats facing dealers and proactive steps to mitigate their risk.

The takeaways from this workshop are:

- ☑ Effective recovery strategies post-disruption
- ☑ Practical steps to enhance disaster preparedness.
- ☑ Broader approaches to manage unexpected challenges.

Understanding Cybercrime

- **Early Ransomware Attacks:**
  - The concept of ransomware began in 1989.
  - The first known ransomware attack involved a single individual distributing infected floppy disks at the World AIDS Conference.
    - When users inserted the disk, it encrypted their files and demanded a ransom of $200 to $300.
  - This early form of cybercrime set the stage for the more sophisticated attacks seen today.
- **Cybercrime as a Business:**
  - Cybercrime has evolved into a highly organized and professional business.
  - These cybercriminal enterprises operate with unlimited manpower, financial resources with call centers and recruitment operations in countries like Russia, China, and Eastern Europe.
  - The infrastructure of these operations is like legitimate businesses, running openly and with extensive resources.
- **Current State of Cybercrime:**
  - **Rising Costs of Cybercrime:**
    - Security professionals agree that the monetary impact of cybercrime is rising.
    - Costs including both direct financial losses and the expenses associated with mitigation and recovery are projected to be $10 trillion in 2024 and $24 trillion in 2028.
  - **Major Cyberattacks in the 1st half of 2024:**
    - **CDK Global:**
      - A significant attack that disrupted operations and highlighted vulnerabilities in the automotive sector.
    - **Findley Auto Group:**
      - Another large automotive group that experienced a prolonged system outage.
    - **United Healthcare:**
      - A major healthcare provider impacted, illustrating the breadth of targets.
    - **Frontier Airlines, ThyssenKrupp, Fujitsu, Prudential Financial:**
      - These companies also faced significant cyberattacks, demonstrating the widespread nature of the threat.
    - **Erik's Mom:** Yes, even individuals, such as Eric Nachbar's mother, have fallen victim to cybercrime, showcasing the personal and varied scope of these attacks.

Many cyberattacks go unreported in the media and Helion Technologies has been involved in remediation for clients who suffered successful cyberattacks.

Cyberattack Consequences

- **Downtime and Lost Revenue:**
  - Cyberattacks can cause significant operational disruptions, leading to downtime.

- Prolonged outages can result in substantial revenue losses, sometimes amounting to millions or even billions of dollars.

- **Reputational Damage:**
  - The public disclosure of a cyberattack can severely harm a company's reputation.
  - Customers may lose trust in the organization's ability to protect their data.
  - Negative publicity can persist online and affect the company's image for years.
- **For example, search results for Findlay Auto Group highlight their cyberattack, potentially deterring customers.**
- **Attack Mitigation and Clean-Up Costs:**
  - Mitigating a cyberattack often requires hiring specialized third-party experts.
  - These costs include identifying and eliminating the threat, restoring systems, and ensuring no further vulnerabilities are present.
  - Post-attack clean-up can be extensive, involving data recovery and system reinforcement.
    - For example, CDK Global had to engage third-party experts for attack mitigation and clean-up, adding to their overall costs.
      - Lawsuits from customers harmed by the breach are not uncommon.
- **Regulatory Accountability:**
  - Organizations are increasingly subject to stringent regulatory requirements regarding data protection and failing to comply with regulations can lead to legal actions, fines, and additional oversight.
  - Examples of regulatory risk
    - All U.S. businesses handling customer information are subject to FTC safeguards.
    - California, businesses must comply with the California Consumer Privacy Act (CCPA).
    - Most states have a variety of laws that can be applied to such breaches.

Opportunities for Improvement

- **Reducing the Attack Surface:**
  - The attack surface refers to all possible entry points through which cybercriminals can gain access to a system.
  - Examples include unauthorized flash drives, Phishing, and other Spam emails to name a few.
- **Strategies:**
  - Regularly update and patch software to close known vulnerabilities.
  - Limit the use of outdated or unsupported technologies that may have security gaps.
    - For example, transitioning from Windows 10 to Windows 11 before the 2025 end-of-support deadline to ensure continued security updates.

- Implement multi-factor authentication (MFA) and strong password policies to reduce unauthorized access.
- Minimize administrative privileges to essential personnel only.

The importance of Understanding IT Infrastructure and Responsibilities:

For better or worse, IT is no longer (and likely never was) an expense item to be controlled.

Because of the substantial downside from breaches and the absence of "quick fixes," robust investment in IT resources is more critical than ever.

Focusing on these areas can significantly enhance the dealership cybersecurity posture, reduce the risk of successful attacks, and ensure compliance with regulatory requirements.

- **IT Team Responsibilities:**
  - Clearly define the roles and responsibilities of IT staff and security personnel.
  - Ensure regular training and certification for IT and security staff to keep up with evolving threats.
- **Policies and Procedures:**
  - Develop and enforce robust security policies, including acceptable use, incident response, and data protection guidelines.
  - Conduct annual security reviews and audits to identify areas for improvement and ensure compliance with regulations.
- **Technologies in use:**
  - Conduct a comprehensive review of current IT systems and processes.
    - Are personal devices being used?
  - Identify all hardware, software, and network components in use.
    - Are they up to date?
    - Were they purchased new or used?
  - Identify vendors and how they operate.
- Opportunities for Enhancement:
  - For example, implementing a federated single sign-on system to centralize user management and simplify access control across multiple systems.
- **Trust but Verify:**
  - Regularly verify that security measures are implemented and followed correctly.
  - Use third-party assessments and penetration testing to gain an external perspective on security posture.

Essential Security Practices

Annual Security Review:

- An annual security review should be performed by certified individuals who have the necessary expertise in cybersecurity, can identify vulnerabilities, assess current security measures, and recommend improvements.

- Certification ensures that the individual conducting the review has up-to-date knowledge and skills.
- The findings and recommendations from the security review should be documented and presented in writing to the board of directors.
- This ensures that senior management is aware of the security posture of the organization and can make informed decisions about necessary investments and improvements.
- Regular reporting to the board promotes accountability and highlights the importance of cybersecurity at the highest levels of the organization.

Realtime Attacker Hunting:

AI can be used to ID suspicious activity in real time and mitigate damage from bad actors.

- **Importance of a Security Operations Center (SOC) and System Log Analytics:**
  - A Security Operations Center (SOC) is essential for monitoring and responding to security incidents in real-time.
  - The SOC uses system log analytics to track and analyze activities across the network, identifying suspicious behavior and potential threats.
  - By continuously monitoring logs, the SOC can detect anomalies that may indicate an ongoing attack.
- **Use of AI for Attack Correlation:**
  - Artificial intelligence (AI) can enhance the effectiveness of threat detection by correlating data from multiple sources.
  - AI can identify patterns and relationships that might be missed by human analysts, providing early warning of coordinated attacks.
  - AI-driven attack correlation helps prioritize alerts and focus resources on the most significant threats.
  - Presented in writing to the board of directors.

Account Security:

- **Audit Administrator Access:**
  - Regular audits of administrator accounts are crucial to ensure that only authorized personnel have elevated privileges.
  - These audits help identify and remove unnecessary or outdated accounts, reducing the risk of misuse.
  - Keeping track of who has admin access and why is a fundamental aspect of maintaining security.
- **Limit PC Admin Access:**
  - Admin access should be restricted to minimize the potential damage if an account is compromised.
  - Employees should have the minimum level of access necessary to perform their duties.
  - Implementing role-based access controls can help manage and enforce these limitations.

- **Secure Passwords and Apply Privileges Sparingly:**
  - Strong, complex passwords are essential for protecting accounts.
    - Erik noted that he still finds easily cracked passwords like "Password2023", "Service1223" etc. on dealership equipment.
  - Password policies should enforce complexity requirements and require regular changes.
  - Privileges should be granted sparingly, and only to those who genuinely need them to perform their tasks.
- **Implement Multi-Factor Authentication (MFA) and Federated Single Sign-On:**
  - Multi-factor authentication (MFA) adds an extra layer of security by requiring additional verification beyond just a password.
  - Federated single sign-on (SSO) simplifies user management and enhances security by centralizing authentication.
  - SSO allows users to access multiple systems with one set of credentials, reducing the number of passwords to manage and secure the authentication process.
- **Keep Technology Current:**
  - Keeping software and hardware up to date is critical for security.
  - Regular updates patch vulnerabilities that could be exploited by attackers.
  - **Avoid End-of-Life technologies** and plan for technology refreshes to ensure all systems meet current security standards.

Employee Training:

- **Importance of Ongoing Security Training and Phishing Tests:**
  - Employees are often the first line of defense against cyber threats.
  - Regular training, upon hire and then at least annually, helps employees recognize and respond to potential security threats, such as phishing attempts.
  - Quarterly phishing tests can evaluate employee awareness and provide additional training where needed.
  - Training should cover security policies, spotting phishing emails, and proper incident reporting procedures.

Penetration Testing (Pen Test) for System Security:

- **Definition and Purpose:** A Penetration Test, commonly referred to as a "Pen" Test, is a simulated cyberattack on a computer system performed by skilled security professionals, known as ethical hackers.

The primary objective of a "pen" test is to identify and exploit vulnerabilities in the system's security defenses and provide a realistic assessment of the system's security posture.

Regular "pe" tests are a crucial component of an organization's cybersecurity strategy.

By proactively identifying and addressing vulnerabilities, organizations can significantly reduce the risk of security breaches and enhance their ability to protect sensitive data and critical assets.

- **Frequency:** It is recommended that organizations conduct "pen" tests annually to ensure that their security measures are up-to-date and effective against the latest threats.
- **Types of "Pen" Tests:**
    - **Black Box Testing:** The tester has no prior knowledge of the target system, simulating an external attack.
    - **White Box Testing:** The tester has full access to the target system's code and configurations, providing a comprehensive assessment.
    - **Gray Box Testing:** The tester has limited knowledge of the target system, representing an attack by an insider or someone with partial access.
- Benefits of "Pen" Testing:
    - **Identify Security Gaps:** Uncover vulnerabilities that could be exploited by malicious attackers.
    - **Improve Security Posture:** Enhance the overall security of the system by addressing identified weaknesses.
    - **Compliance:** Meet regulatory and industry standards that require regular security assessments.
    - **Risk Management:** Prioritize security investments by understanding the potential impact of vulnerabilities.
    - **Incident Response:** Improve the organization's ability to detect and respond to security incidents.
- Components of a "Pen" Test:
    - **Objective Setting:** Define the scope, goals, and rules of engagement for the test.
    - **Information Gathering:** Collect information about the target system, such as network architecture, operating systems, and software applications.
    - **Scanning:**
    - **Static Analysis:** Inspect the target system's code and configurations for vulnerabilities without executing it.
    - **Dynamic Analysis:** Evaluate the target system's behavior during runtime to identify potential security flaws.
- Gaining Access:
    - **Exploitation:** Use the identified vulnerabilities to gain unauthorized access to the system.
    - **Privilege Escalation:** Attempt to escalate privileges to higher levels, such as administrator or root, to assess the extent of potential damage.
- Maintaining Access:
    - **Persistence:** Establish a foothold in the system to ensure continued access even after reboots or other system changes.
    - **Backdoors:** Install backdoors or other mechanisms to regain access if the initial entry point is closed.

- **Analysis and Reporting:**
  - **Documenting Findings:** Record all vulnerabilities discovered, along with details of how they were exploited.
  - **Risk Assessment:** Evaluate the impact and likelihood of each vulnerability being exploited in a real-world scenario.
  - **Recommendations:** Provide actionable recommendations for mitigating identified vulnerabilities.
- **Remediation and Retesting:**
  - **Fixing Vulnerabilities:** Implement the recommended security measures to address the discovered weaknesses.
  - **Verification:** Conduct a follow-up test to ensure that the vulnerabilities have been successfully mitigated.

Vulnerability Scan: Semi-Annual Scan and Patching of Computer Systems

Definition and Purpose: A vulnerability scan is an automated process that systematically examines a computer system, network, or application to identify potential security weaknesses.

These scans are designed to detect known vulnerabilities such as outdated software, missing patches, misconfigurations, and weak passwords.

The primary purpose of conducting vulnerability scans is to identify and address security issues before they can be exploited by malicious actors.

Be aware that automated scans may produce false positives, which need to be manually verified.

- **Frequency:** Semi-annual (twice a year) vulnerability scans are recommended to ensure continuous monitoring and timely remediation of security vulnerabilities.
- Components of a Vulnerability Scan:
  - Planning and Preparation:
    - **Scope Definition:** Determine the scope of the scan, including the systems, networks, and applications to be assessed.
      - **Asset Inventory:** Compile a list of all assets within the scope, such as servers, workstations, network devices, and software applications.
      - Ensure that all critical assets are included in the scan scope to avoid blind spots.
  - **Scanning:**
    - **Automated Tools:** Utilize specialized vulnerability scanning tools that can automate the process of identifying security weaknesses.
    - **Network Scanning:** Examine network infrastructure for open ports, services, and potential vulnerabilities.
    - **Application Scanning:** Assess web applications and software for common security flaws such as SQL injection, cross-site scripting (XSS), and insecure configurations.
    - **Credentialed Scanning:** Use administrative credentials to perform a more in-depth assessment of system configurations and installed software.

- **Analysis and Prioritization:**
  - **Vulnerability Identification:** Identify and catalog all discovered vulnerabilities, including their severity and potential impact.
  - **Risk Assessment:** Prioritize vulnerabilities based on factors such as exploitability, potential impact, and the criticality of the affected assets.
- **Reporting:**
  - **Detailed Reports:** Generate comprehensive reports that outline the identified vulnerabilities, their severity, and recommended remediation steps.
  - **Executive Summaries:** Provide high-level summaries for management, highlighting the most critical issues and overall security posture.
- **Remediation:**
  - **Patch Management:** Apply security patches and updates to address identified vulnerabilities in software and operating systems.
  - **Configuration Changes:** Implement configuration changes to harden system security, such as disabling unnecessary services and enforcing strong password policies.
  - **Verification:** Conduct follow-up scans to verify that vulnerabilities have been successfully mitigated.
- **Benefits of Vulnerability Scans:**
  - **Proactive Security:** Identify and address vulnerabilities before attackers can exploit them.
  - **Regulatory Compliance:** Ensure compliance with industry regulations and standards that require regular security assessments.
  - **Risk Management:** Improve risk management by understanding and mitigating potential security threats.
  - **Continuous Improvement:** Enhance the overall security posture through regular monitoring and remediation of vulnerabilities.

Insurance Coverage:

- **Accurate Representation in Insurance Applications:**
  - When applying for cyber insurance, it is crucial to accurately represent the security measures in place.
  - Misrepresentations can lead to denied claims or legal issues if a breach occurs.
  - Ensure that all information provided to insurers is accurate and up to date.
- **Importance of Having a "Breach Coach" and Understanding Coverage Specifics:**
  - A Breach Coach can guide the organization through the response process during a cyber incident.
  - Understanding the specifics of the insurance coverage, including what is and isn't covered, is vital.
  - Be aware of coverage limits, deductibles, and the support services provided by the insurer.
- By implementing these essential security practices, organizations can significantly enhance their cybersecurity posture, reduce vulnerabilities, and ensure compliance with regulatory requirements.

Conclusion

When asked during Q&A whether a DMS or CRM provider that runs in the cloud provides more or less protection Erik stated that generally the answer is "more" because cloud servers such as Microsoft, etc. have greater resources than are available to dealerships, Helion Technology, etc.

In closing, Erik stressed that there are no quick fixes in cyber-security because the cyber-criminals have us outgunned in manpower and resources. However ongoing vigilance and preparation reduces the odds of becoming a victim and can mitigate the damage that an attack can inflict.

Erik offers a free IT assessment and can be reached at:

Enachbahr@heliontechnologies.com

443-610-7640

www.HelionTechnologies.com/it-assessment