CDK™ Cybersecurity

# Three Steps to Incident Readiness

## HOPE FOR THE BEST BUT PREPARE FOR THE WORST

Improve cybersecurity outcomes by preparing your dealership IT Security team to respond quickly and effectively.

nuspire

This white paper was created in partnership with Nuspire and CDK Global.

# Rapid Effective Incident Response Begins With Incident Readiness

IT security incidents will happen. The certainness for uncertainty, on account of their timing and techniques being unknown, stretches security teams thin while doing their best to secure your dealership. Unfortunately, many priorities within your store demand time and attention. Reactive, unplanned, unrehearsed incident response can delay threat identification, containment and remediation. Your dealership's security team can reduce this risk by following these three steps: prepare, practice and test.

## THREE STEPS TO INCIDENT READINESS

Game plans exist for a good reason. They work because they minimize uncertainty, confusion and guesswork. By following the right game plan, your dealership can assemble a security team that's ready to leap into action to reduce threat response time and malicious activities.

1 Prepare

2 Practice

3 Test

STEP ONE:

# Prepare

An incident response plan details, at a minimum, the participants and their roles and responsibilities. Superior plans are usually customized and based on a recognized standard such as NIST. Your cybersecurity vendors should help you develop a plan and gather information to shape your plan. Information gathering begins with interviews, a threat landscape assessment and industry-specific threat modeling. These activities form a picture of your environment and requirements, your dealership's exposure on the internet and a view of high-priority adversaries. Additional plan development activities include:

## IDENTIFYING KEY PLAYERS

An on-call roster specifically for cybersecurity events allows your dealership to respond to incidents faster. The roster should identify an Incident Commander and other team leads who can take charge of an incident.

## CREATING A PROCESS FOR WORKING AN INCIDENT

A well-defined process allows the Incident Commander to understand what resources are available and how to use them. The process details each team's steps and actions to complete response tasks as directed by the Incident Commander.

## INDUSTRY-SPECIFIC THREAT MODELING

**The outcomes of threat modeling help you make the best use of limited staff and resources:**

- Learn which threat techniques are most relevant to the automotive industry and your dealership
- Understand where to expand or optimize controls and protection
- Detect and block attacks before they do harm
- Fortify defense related to your most valuable assets

As time goes on, it appears that attackers become increasingly efficient and lean more toward attacks such as phishing and credential theft[1].

### BEST PRACTICE

Balance humans and technology to understand the threat landscape and use threat intelligence effectively.

**Actions to take when you are attacked:**

- Execute your IR plan
- Disconnect affected workstations from the network
- Contact your cyber insurance company
- Contact your trusted cybersecurity partners
- Do not try to collect forensics — leave that to the experts
- Ready your processing backup plan for connectivity
- Await instruction from your insurance company and trusted partners

STEP TWO:

# Practice

Rehearsing your plan reveals what's working or not working, so the plan can be fine-tuned before an incident occurs. The following exercises allow individuals to hone their skills while reinforcing the importance of collaboration:

## PURPLE TEAM TECHNICAL ASSESSMENT

Your security practitioners and external cybersecurity experts participate in customized, simulated incidents drawn from your industry's threat landscape. Participants follow your plan and playbook to respond to internal or external threats. This activity often uncovers issues such as improperly configured alerts, underprotected credentials and weak passwords. Automated red-teaming tools can be incorporated into assessments.

## SCENARIO-BASED TESTING

A scenario such as security awareness training focused on phishing helps prepare your associates for business compromise attempts. The goal is to find out how likely it is that users will be tricked into interacting with a malicious email or providing sensitive information via phone or text. A scenario may include sending an email that appears to be from IT. The email contains instructions to visit a link, download a tool, enter a code and enable access. Results are summarized in a report. Follow-up training teaches employees to identify suspicious communications, follow defined procedures and get the security team involved.

## TABLETOP EXERCISES

Individuals participate in paper-based scenarios that include relevant threat intelligence, an incident like ransomware or another upward-trending threat. Participants walk through capabilities, roles, responsibilities and response options. Initial tabletop exercises may involve the Director of IT, General Manager and owners at your dealership.

### BEST PRACTICE

Conduct practice assessments, testing and exercises frequently. Aim to complete at least one activity per quarter.

**Social actions arrived via...[2]**

| 96% | 3% | >1% |
|---|---|---|
| Email | Website | Phone/SMS |

RANSOMWARE ACTIVITY PEAKED DURING WEEKS 9 AND 10 OF Q4, TOPPING OUT AN **INCREASE OF MORE THAN 10,000%.[3]**

STEP THREE:

# Test

Testing helps you find and fix exploitable security vulnerabilities. Reports include recommended remediation actions and information that may be relevant to incident readiness planning. Additionally, the findings from the following activities are excellent talking points in risk management discussions:

## VULNERABILITY ASSESSMENT

Automated scanning helps identify, classify and prioritize security weaknesses throughout your environment. Assessments reveal vulnerabilities such as privilege escalation attacks that can be countered with password policies, elevated credential management or other controls.

## PENETRATION TESTING

A simulated cyberattack tests your security controls and uncovers issues such as system configuration errors, open ports, weak passwords and software flaws.

## COMMON USES OF PENETRATION TESTING

**Investigate whether data being transferred among systems or over networks is secure.**

- ✓ **Launch a social engineering attack that attempts to capture sensitive information.**
- ✓ **Check the security of web applications or other software programs.**

**With cloud platforms…identity and credential management of administrators, cloud instances, and storage configuration are not only easy and quick to configure, they are also easy to misconfigure.** [4]

### BEST PRACTICE

Automate and conduct weekly vulnerability scans. Pass the results to penetration testers, who can devise and execute targeted, simulated attacks.

# Final Thoughts

### Keep Your Eyes on the Prize: Reducing Incident Time

Incident readiness can be sidelined by a lack of time, skills and budget. Given the certain uncertainty of the threat landscape within the automotive retail space, security leaders at your store should prepare for the worst.

**Preparing, practicing and testing your incident readiness empowers your dealership** to reduce incident resolution time, adversary dwell time and damage to your reputation and bottom line.

As you evaluate incident readiness providers, you should look for a vendor that can provide various levels of support for deeper investigation and analysis. Your vendor should also be able to offer guidance on containment, remediation and future mitigation. [5]

## ABOUT CDK GLOBAL INC.

With approximately $2 billion in revenues, CDK Global (NASDAQ: CDK) is a leading provider of retail technology and software as a service (SaaS) solutions that help dealers and auto manufacturers run their businesses more efficiently, drive improved profitability and create frictionless purchasing and ownership experiences for consumers. Today, CDK serves over 15,000 retail locations in North America. For more information, visit **cdkglobal.com.**

## ABOUT NUSPIRE

Nuspire is a leading managed security services provider (MSSP) that is revolutionizing the cybersecurity experience by taking an optimistic and people first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24x7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine award winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser focused on delivering an extraordinary cybersecurity experience that exceeds client expectations. For more information, visit **www.nuspire.com** and follow **@Nuspire**.

## RESOURCES

1. Verizon, Data Breach Investigations Report, 2020.

2. Ibid.

3. Nuspire, Threat Landscape Report, Q4 2020.

4. Forrester, Assess Your Cloud Security Readiness, May 29, 2020.

5. IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment.

CDK GLOBAL®

Learn more at **CDKGlobal.com**