Defending Against Cyber Attacks What to Expect in 2023

By David Shluger, Vice President Cyber Risk Engineering
Zurich Resilience Solutions

Cybercrime has become an incredibly lucrative business for threat actors and hackers. The risk picture for auto dealers in 2023 reveals emerging cyber schemes as well as the tried-and-true tactics threat actors have used for many years. Here's how to best protect your dealership and defend against cyber attacks.

The major risks we saw in 2022

1 Business Email Compromise:

Cybercrime in which a scammer uses email to trick someone into sending money or divulging confidential company information.

Recent attack: A financial services firm confirmed that the company experienced a data breach after an unauthorized party gained access to sensitive consumer data contained on their network through an email-based cyber attack.

Fifteen percent of car dealers have experienced a cyber security incident in the past year. Of those impacted, 85% of the occurrences were due to sophisticated phishing attempts concealed as legitimate emails that resulted in data breaches, IT-related business interruptions, and loss of revenue.

Source: https://www.jdsupra.com/legalnews/acorn-financial-services-reports-data-5996771/

2 Ransomware:

Malicious software that encrypts data and systems, holding them hostage for ransom.

Recent attack: A classic ransomware attack was perpetrated on an automotive group in Florida in 2022 which ultimately cost the dealership an estimated $500K including 250 new computers, consulting services of external security response experts, and upgraded security software.

Ransomware is among the most lucrative hacking tactics and will likely remain one of the greatest threats to dealerships of every size for the foreseeable future.

3 Third Party Impacts:

A supplier, vendor, customer, or other "trusted" third party falls victim to a cyber incident and it has downstream impacts.

Recent attack: In February 2022, a major OEM announced that it was forced to stop car production operations after a major supplier suffered a data breach.

In October 2022, the OEM's customers suffered another data breach after a contractor developing the brand's official connectivity app left a repository containing client data publicly exposed.

Source: https://www.bleepingcomputer.com/news/security/toyota-halts-production-after-reported-cyberattack-on-supplier/

Trends and predictions for the 2023 risk picture

Crime-as-a-Service

The cost of global cybercrime has been estimated by market and consumer data company, Statista, to reach $10.5 trillion by 2025. This is supported by blockchain analysis firm, Chainalysis, reporting that cybercriminals have stolen more than $3 billion in crypto-based cyber attacks between January and October of 2022 alone.

Third-Party Risks

With the advent of cloud migration, companies are increasingly incorporating third-party software solutions into their infrastructure. Many cyber security professionals are wary of the risks incurred by this decision, and more than a third (36 percent) of those reporting to Cyber Security Hub say that supply chain/third-party risks are a top threat to their organization's cyber security.

Human error

With the advent of cloud migration, companies are increasingly incorporating third-party software solutions into their infrastructure. Many cyber security professionals are wary of the risks incurred by this decision, and more than a third (36 percent) of those reporting to Cyber Security Hub say that supply chain/third-party risks are a top threat to their organization's cyber security.

Human error is predicted to remain a major factor in cyber security threats for 2023. In 2022, research by the World Economic Forum found that 95 percent of cyber security issues could be traced back to human error. Likewise, almost a third of cyber security professionals (30 percent) told Cyber Security Hub that lack of cyber security expertise was the number one threat to cyber security at their organization. The types of human errors in cyber security can be categorized into skill-based and decision-based errors.

- Skill-based errors are generally minor errors that occur while carrying out a daily task.
- Decision-based errors result from a lack of knowledge, skills, and information about a specific circumstance.
- Unauthorized access to a computer or an account can give another user straight access to confidential information. Physical security errors often take place when a device is left unattended.

Defending against cyber attacks *Continued*

How can you defend your dealership?

Top 10 Cybersecurity Controls of 2023

1. Encryption

A data-centric security strategy focuses on protecting data at rest, in transit, and in use, protecting your data when it's on your network, sent anywhere within your network, or outside your company. This strategy encompasses elements of data discovery, access management, data protection, loss prevention, data governance, and compliance.

2. Connected devices

Cyber security for operational technology (OT) and Internet of Things (IoT) is a field of study and practice to prevent the unauthorized access, manipulation, and disruption of OT and IoT devices/platforms. Cyber security programs for OT and IoT are commonly independent from IT cyber security programs, but many controls and objectives overlap.

These devices can be very tough to protect because they were never designed to be networked. The most common solution for connected devices is segmentation of your network.

3. SOC monitoring

A Security Operations Center (SOC) is a centralized function provided to an organization that employs people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cyber security incidents. This function, especially those under-resourced, can be enhanced and achieve a higher level of effectiveness with the addition of artificial intelligence (AI).

4. Risk Management

Governance, Risk, and Compliance (GRC) is a structured way to align IT with business goals while managing risks and meeting all industry and government regulations. It includes tools and processes to unify an organization's governance and risk management functions with technological innovation and adoption. Companies use GRC to achieve organizational goals reliably, remove uncertainty, and meet compliance requirements.

5. Security and Awareness Training

Humans are the weakest link in any cyber security program. The purpose of security awareness and training is to educate users on how to identify, report, and prevent potential cyber attacks such as phishing and social engineering. A well-designed security awareness and training program uses a variety of delivery formats to create a strong security culture. These formats include, but are not limited to, mandatory training at hire and at least annually thereafter, regular phishing exercises, and periodic reminders.

6. Zero Trust

Zero Trust is a security framework requiring all users, whether on or off an organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture in order to obtain and maintain access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or follow a hybrid model.

7. Identity and Access Management

Identity and Access Management (IAM) is performed by implementing business processes, policies, and technologies to manage identities, roles, access rights, and authentication protocols. This includes those for users, administrators, third parties, etc., irrespective of location.

8. Cloud Security

Cloud security is a collection of procedures and technology designed to address external and internal threats to an organization's cloud-based resources. Organizations need cloud security as they move toward their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.

9. Email Security

Email security is a term for describing different procedures and techniques to protect email accounts, content, and communication against unauthorized access, data loss, or compromise. Email is often used to spread malware, spam, and phishing attacks.

Web security refers to the protective measures and protocols used to protect an organization from cyber criminals and threats that use the web channel.

10. Business Continuity and Disaster Recovery Planning

Though often used interchangeably, business continuity and disaster recovery are different processes with unique goals.

- Business Continuity (BC): Keeping critical business operations and functions running during a disaster.
- Disaster Recovery (DR): Restoring data and IT systems after a disaster.

Only by combining the two processes, along with a strong data backup strategy, can organizations comprehensively prepare for and limit the impact of a disaster.