CASE STUDY

AUTOMOTIVE CYBER SECURITY RISK

In 2016, a New Jersey-based chain of auto dealers suffered a damaging cyber-attack when an employee, who was surfing the internet on his lunch break, unknowingly visited a malicious website.

The website exploited an outdated web browser on the employee’s computer and infected the machine with a type of malware called ransomware. The malicious software spent the next six days quietly taking control and encrypting all of the files on the infected computer, as well as all of the files on the dealership’s network server. Once the software finished encrypting the files, an on-screen message demanded thousands of dollars be sent to the hackers. If the payment was not made within 48 hours, the files that were now under the attackers control would be lost forever, including critical data needed for operations.

The dealership’s IT personnel tried unsuccessfully to eradicate the infection, and the network was down for two days, affecting the dealer’s ability to operate. In the end, the dealership was forced to pay the ransom, and the incident was a huge distraction to the business, even affecting their sales numbers for the month.

Companies in the automotive industry falling victim to hackers is a growing issue. Incidents of hacking and cyber-breaches are on the rise across all industries and for companies of all sizes. Automotive dealerships and vendors face the standard cyber-risks that all industries with internet-facing systems are exposed to, but they also face unique risks based on the nature of their work and the data that they possess, as outlined herein.

This case study seeks to outline the issues we have found and bring further attention to these risks and the need for action by those organizations who are not fully cognizant of this issue or who falsely assume they are safe.
WithumSmith+Brown, PC (Withum), a cybersecurity provider, has seen these issues first-hand. We have performed proactive security assessments and penetration tests for forward-thinking automotive industry clients, and have been involved in cyber-breach incident response for companies who have already fallen victim to malicious cyber-attacks.

In performing our security assessments, Withum has found that, almost uniformly, our automotive industry clients have had vulnerabilities in their systems that would allow malicious attackers to gain access to a dangerous set of data, including:

- Access to company records, including financials, partner compensation, payroll records, employee social security numbers and confidential information.
- Access to customer records, including confidential financial information that dealerships are required by law to keep protected.
- Ability to access banking and financial accounts, transfer money out, and re-route inbound funds.
- Access to IT administrator accounts, allowing full control of networks and all resources.
- Access to user accounts, including emails, network access, and all assigned capabilities.
- Full control over networks, devices, phone systems, and security systems.

Having access to all of these items at once is obviously troubling and it could be severely damaging in the wrong hands. Damages could include financial losses, law suits, government-imposed fines, embarrassment, and job loss. All of the access and information was gained remotely, without our team of experts ever setting foot in the facilities. Thankfully, we are trusted professionals and we were able to provide remediation steps to our clients to close the security gaps and limit the likelihood that these attacks would occur in the real world. Unfortunately, we are concerned that far too many law firms are not taking the proper steps to prevent similar attacks. The issue looks to only be getting worse as attackers recognize the pervasiveness of vulnerabilities and caches of valuable data in this industry.

The issue looks to only be getting worse as attackers recognize the pervasiveness of vulnerabilities and caches of valuable data in this industry. This data can be used for other crimes, such as opening a fraudulent credit account in the victim’s name. The data can also be sold on the black market.
UNIQUE FACTORS AFFECTING THE AUTOMOTIVE INDUSTRY

Besides the standard risks inherent to all industries with internet-facing systems, auto dealerships and other businesses serving the auto industry face additional threats due to the volume and types of data that they typically house. Hackers may specifically target businesses in this industry due to the troves of customer data that often reside on their systems, such as financials, credit applications, credit scores, social security numbers, etc.

Hackers have also come to realize that many automotive industry businesses have very weak defenses and can be easily breached. Hackers know they can get in and remain undetected for extended periods of time, even permanently, and quietly exfiltrate valuable data and use it for their malicious gains. A large volume of valuable data mixed with traditionally poor defenses make for a bad combination.

Auto industry information systems typically have numerous external entry points, as connections are setup to other systems such as manufacturers, suppliers, other departments, etc. Your typical auto dealership has computers everywhere; at the sales desks, at the receptionist, in the part and labor departments, and even at the shop bays.

There is almost always “Free Wi-Fi” offered to customers, and all the systems are usually not properly segregated, meaning a skilled attacker can penetrate into the network and access confidential information with relative ease. Also troubling, systems are often outdated, not maintained, or part of a legacy infrastructure, such as dial-up remote connections, and sometimes legacy entry points are forgotten and left open. Auto dealerships essentially have the networks and data of large sophisticated corporations, but typically the security and savvy of a much smaller business.

Another huge threat faced in this industry is wire transfer fraud. Large financial transaction and movement of five to six digit funds is not unusual in automotive companies. Hackers will target weaknesses in process and procedure to social engineer wire transfer fraud and other theft of funds, or directly steal banking credentials and initiate and approve the transfers themselves. These types of attacks are occurring in record numbers, and the money is often unrecoverable.

In an industry that relies heavily on customer service, reputation, referrals and repeat business, the black-eye that can come from being hacked and breaching customer data can have long-lasting and severely damaging effects. Dealers could even face penalties for legal violations or civil lawsuits for failure to protect sensitive information on their customers, including their financial data.

AUTOMOTIVE CYBER SECURITY RISK TEAM
Joseph Riccie  
T (609) 514 5597  
jriccie@withum.com

Sumit K. Pal  
T (609) 514 5595  
spal@withum.com

Anurag Sharma  
T (609) 945 7985  
asharma@withum.com

withum
AUDIT TAX ADVISORY
HOW TO MITIGATE RISK?

There are a few basic steps law firms should be taking to help mitigate this risk:

<table>
<thead>
<tr>
<th>STEP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cybersecurity cannot simply be relegated to IT. Have an Information Security Committee that meets regularly and includes key personnel and staff from upper management and relevant departments.</td>
</tr>
<tr>
<td>2</td>
<td>Have a written Information Security Program, with documented policies and procedures, as well as risk analyses and contingency plans.</td>
</tr>
<tr>
<td>3</td>
<td>Have a Penetration Test performed annually by an independent security firm, and ensure the remediation steps that come from the test are actuated.</td>
</tr>
<tr>
<td>4</td>
<td>Train all staff on Cybersecurity Awareness. Many hackers try to bypass strong technical defenses by compromising unknowing employees who have access to your systems.</td>
</tr>
<tr>
<td>5</td>
<td>Use strong and unique passwords and enable two-factor authentication whenever possible.</td>
</tr>
<tr>
<td>6</td>
<td>Ensure backups are performed daily for critical data and stored off-site, such as with a cloud service provider.</td>
</tr>
<tr>
<td>7</td>
<td>Allocate the proper funds for cybersecurity.</td>
</tr>
</tbody>
</table>

WHAT IS A PENETRATION TEST?

A Penetration Test is a security exercise where a team of highly-trained security experts attempt to hack into the client’s network in order to find security weaknesses.

The intent is to discover ways that a real-world attacker might be able to compromise the systems. The highly-trained security team is careful not to cause any actual harm and a report is provided detailing all of the vulnerabilities and weaknesses found and outlining exactly what needs to be done to fix them.

In-house IT staff are usually pressured to make things functional and easy-to-use, which diametrically oppose security. Also, it is difficult for an organization’s own IT staff to objectively look at their own systems from an outsider’s perspective. Just like a CFO needs a CPA firm to review their financials, senior IT leadership benefits from having a team of certified security experts independently test their system to give them valuable insight.
WITHUM CYBER SECURITY RISK TEAM

Joseph Riccie, CPA, Partner, Market Leader
Cloud Solutions & Management Consulting
Joe has over 30 years of financial, human capital and operational management experience collectively. Joe is a proven, results-driven, entrepreneurial professional focused on improving the financial, human capital and operational management activities for companies across a variety of industries. He specializes in managing programs, leading change enablement and enterprise transformation programs, and he has a recognized ability to leverage people, process, technology and information to drive performance and deliver key business objectives with tangible results.

Sumit K. Pal, CGEIT, CISA, MBA, Principal
Cyber Security & Information Technology Services
Sumit is certified in the governance of enterprise IT (CGEIT), and Risk and Information Systems Control (CRISC), and is a certified information systems auditor (CISA). Sumit has more than 27 years of professional experience in business consulting and systems integration. He is responsible for the firm’s IT audit and data analytics services. He is also the team leader for the Intellectual Property and Royalty Audits niche. Sumit’s areas of expertise include Sarbanes-Oxley Section 404 projects, IT audits, IT internal control assessments, operational reviews, Service Organization Controls (SOC), internal auditing, business process analysis, business process documentation and re-engineering.

Anurag Sharma, CISA, CISSP, CRISC, MBA, Principal
Cyber Security & Information Technology Services
Anurag is a Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), and Certified in Risk and Information Systems Controls (CRISC). He is also designated as a SOC 1 and SOC 2 specialist by the Oversight Task Force of the AICPA Peer Review Board. He has over 16 years of experience and is one of Withum’s leading IT audit specialists. His areas of expertise include Cybersecurity Assessments (NIST Cybersecurity Framework), SSAE 16 (SOC 1) Audits, SOC 2 Audits, Information Security Consulting, Corporate Governance, Sarbanes-Oxley Section 404 compliance and ISO/IEC 27001 Consulting.