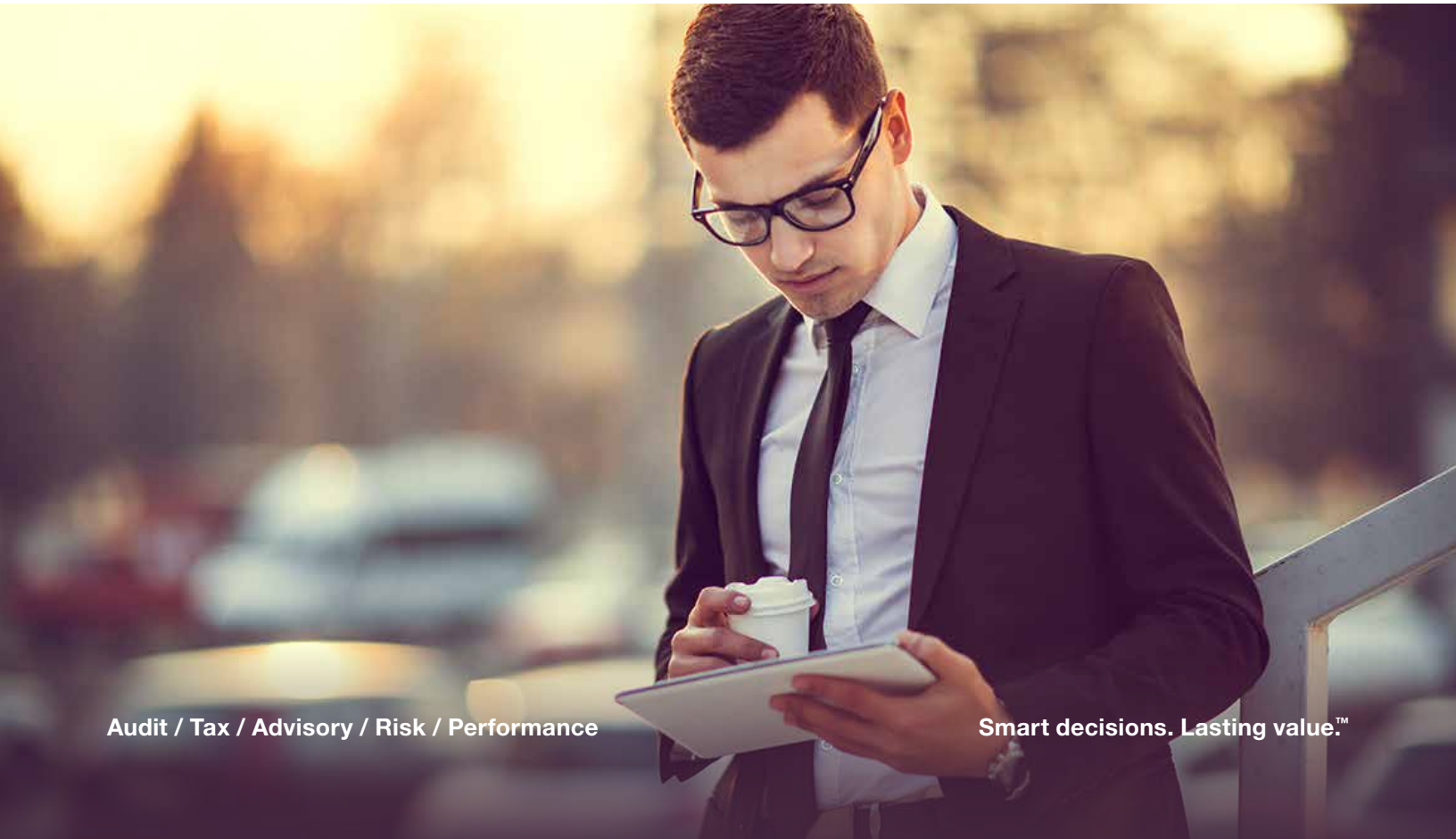
Crowe

August 2017

Cyber Resilience for Retail Dealers

Going Beyond Security to a New Level of Readiness

An article by Mike Del Giudice, CISSP, CRISC; Gregory Dougherty, CPA; and Chris Wilkinson, CISSP, CRISC



In recent years, the term “cyber resilience” has become common in discussions about cybersecurity, risk management, and breach mitigation. Cyber resilience represents a different and useful way of thinking about protecting data and information systems.

Rather than focusing only on preventing attacks or intrusions on retail dealer systems, cyber resilience also attempts to mitigate the consequences of such incidents. As attacks on data and information systems increase – and become increasingly malicious – the concept of cyber resilience can help organizations of all types and sizes do a better job of minimizing the damage caused by these attacks.

Today’s Threat Environment

Cybersecurity has been a serious concern in both the public and private sectors for quite some time, but the level of concern has increased in recent years as new types of threats emerge. Among the most pervasive of the current generation of threats are ransomware (malicious software that blocks access to a system or data until a sum of money is paid) and whaling (targeted scam emails that appear to be from a high-level executive or other legitimate authority).

Threats such as these are not only more difficult to detect than earlier types of incidents but also more malicious in their intent and more devastating in their potential effects. Their consequences are often immediate and severely damaging.

For example, the newest types of ransomware no longer merely hold a company’s data hostage until a ransom is paid; they actually start destroying data if the ransom isn’t paid quickly.[1] One research study shows that almost 40 percent of companies experienced a ransomware event in the 12 months preceding August 2016,[2] and based on estimates from the FBI, over $200 million dollars was paid to ransomware criminals in the first quarter of 2016.[3]

Moreover, all signs point to attackers continuing to target underprotected assets. Consider, for example, the November 2016 breach of DealerBuilt, in which names, addresses, and social security numbers of customers and employees of dealers were exposed online.[4]

Not Whether but When

Most security experts have come to recognize that cyberattackers have become more numerous, more persistent, and cunning enough to make prevention of an incident alone an inadequate strategy. Some dealerships also are recognizing the near-certainty that some of the attackers' attempts will succeed.

In other words, it's no longer a question of whether an attack will succeed, but when. So what steps can an organization take to minimize the effects of the attack?

That outlook is the underlying mindset that drives organizations to embrace cyber resilience – a concept that draws together practices related to security, disaster recovery, business continuity, and incident response. Many organizations view these disciplines as related but distinct from each other.

However, cyber resilience integrates principles and practices from all these fields into a comprehensive readiness and response strategy aimed at minimizing the damage when an incident occurs.

Cyber Resilience Models and Related Standards

Much of the thinking behind cyber resilience can be traced back to work done for and by the United States Computer Emergency Readiness Team (US-CERT), a division of the U.S. Department of Homeland Security. Working with Carnegie Mellon University's Software Engineering Institute, the team created the CERT Resilience Management Model (CERT-RMM) in 2010, to converge various risk management activities – such as security, business continuity, and IT operations – into a single model. A year later, US-CERT produced the Cyber Resilience Review (CRR), a nontechnical assessment tool to help organizations evaluate operational resilience and cybersecurity practices.

The CERT-RMM and CRR align closely with the central tenets of the widely used National Institute of Standards and Technology (NIST) Cybersecurity Framework. The CRR enables an organization to relate its cyber resilience capabilities to the NIST framework using a document called a "crosswalk" to compare the two approaches and map the features they have in common.

Components of Cyber Resilience

As updated in 2016, the CERT-RMM organizes cyber resilience into 26 separate process areas. The CRR condenses these areas into 10 domains:

1. **Asset management** – Establishment of an inventory of high-value assets grouped into four broad categories – people, information, technology, and facilities – and definition of how these assets are managed to support the organization's critical services
2. **Controls management** – Identification, implementation, and assessment of the administrative, technical, and physical controls used to maintain mission-critical services and assets
3. **Configuration and change management** – Continuous process of controlling and approving changes to information or technology assets or changes to related infrastructure
4. **Vulnerability management** – Processes used to identify, analyze, and address any physical or operational feature that could make the organization susceptible to risk from a natural event or human threat
5. **Incident management** – Improvement of the processes used to detect, identify, evaluate, and respond to events that disrupt critical infrastructure or services
6. **Service continuity management** – Identification of the services most important to carrying out the organization's mission plus the design, development, validation, and testing of service continuity response plans
7. **Risk management** – In the context of cyber resilience, the processes that identify and analyze operational risk to IT-dependent assets and services, and the determination of how to deal with those risks (avoiding, accepting, transferring, or mitigating) in ways that reflect the organization's risk tolerance
8. **External dependencies management** – Management's establishment of the appropriate controls to protect assets and sustain critical activities that depend on relationships with external organizations
9. **Training and awareness** – Education of staff members to give them the knowledge and skills to perform their work in incident management, controls management, risk management, and other related domains
10. **Situational awareness** – Provision of accurate and up-to-date information for stakeholders about the immediate operational condition of critical services so that they can make decisions effectively

These 10 domains provide a helpful framework for understanding the concept of cyber resilience. They also provide dealerships with a structure useful for organizing their cyber resilience efforts. When related to the NIST or a comparable framework, the 10 domains can help risk managers and other responsible parties plan how to deploy their assets – including people, processes, and technology – in support of specific operational missions or critical services.

Moving Beyond Effectiveness to Maturity

It is important to avoid the natural tendency to regard the CRR as a checklist or compliance standard. Rather than approaching cyber resilience with a compliance mindset, it's more useful for an organization to use the assessments to advance its cyber resilience toward greater maturity. The difference is more than just a matter of semantics.

A checklist focuses solely on whether a control objective is being met. It does not question how it is being met, just that it is operating effectively at a given point in time. For example, an organization might have a requirement to patch its systems, and confirmation that those patches are deployed shows that the control objective is met.

Maturity, on the other hand, encompasses not only effectiveness but also two additional important attributes: efficiency and responsiveness.

Say, for example, that an organization establishes a series of manual activities that must be performed as part of its patch management protocol. Such a manual arrangement might be perfectly acceptable and deemed effective, but it does not necessarily reflect a high level of maturity. A more mature organization might choose to automate those same processes in order to go beyond effectiveness to become more efficient or reduce opportunities for errors or oversights as well as become more responsive to change.

Implementing a Cybersecurity Resilience Program

As with all cyber-based programs, the risk and threat landscape is broad and continually maturing, often at a quicker pace than internal responses to those threats. The most effective approach to managing such risks is to start with a comprehensive risk assessment in order to identify which areas to address to provide the most value to the organization.

The risk assessment will identify the cyber resilience components that would be the most advantageous for a dealership to address in the short term, while also providing a general road map for the dealership as the program matures. For example, organizations with little reliance on third parties would see less value in focusing on external dependencies management than would a company that has outsourced critical business systems.

Absent a risk assessment, there are critical components that all dealerships should focus on in the short term:

The most effective approach to managing cybersecurity risks is to start with a comprehensive risk assessment in order to identify which areas to address to provide the most value to the organization.

1. **Incident management** – Cyber resilience is based on the concept that a breach will happen eventually, and the ability to respond to an incident effectively is a critical component of any resilience program. Organizations should proactively identify a formal program and response team, including training and testing exercises to improve efficacy of the program.
2. **Vulnerability management** – Organizations must have visibility into the vulnerabilities in the existing environment in order to manage them appropriately. The ability to mitigate these vulnerabilities, whether through available system patches or other mitigating techniques, greatly decreases the likelihood of an incident becoming a breach.
3. **Training and awareness** – The weakest point of any security effort is typically the end user, which is why phishing continues to be a threat vector that has led to some of the most widely publicized breaches. Most organizations have training programs, but they must determine if these programs actually increase awareness or just “check the box.”
4. **Controls management** – Controls management is a broad topic that requires constant attention. Initially, however, the focus should be on managing those risks related to advanced endpoint protection. In reality, managing employee behavior in the face of advanced phishing schemes is difficult and, even with critical training, incidents will still occur. Organizations need to evaluate technical controls at the endpoints to minimize the impact of an incident when it does occur.

More Than Compliance

By approaching cyber resilience from the perspective of maturity, rather than just effectiveness, those involved can help make cyber resilience efforts more than just another compliance effort. By establishing a foundation for improved decision-making, they can even help cyber resilience develop beyond its primary function, which is being an important risk management tool. By helping a dealership be ready for an incident, a cyber resilience program can limit the impact, increase business continuity, and speed up recovery – ultimately adding value to the organization.

Learn More

Mike Del Giudice
+1 630 575 4359
mike.delgiudice@crowe.com

Chris Wilkinson
Principal
+1 214 777 5288
christopher.wilkinson@crowe.com

Greg Dougherty
Partner
+1 813 209 2406
gregory.dougherty@crowe.com

This article was published originally by Dealer Magazine in August 2017.

---

[1] Lawrence Abrams, "Jigsaw Ransomware Decrypted: Will Delete Your Files Until You Pay the Ransom," BleepingComputer, April 11, 2016, http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/

[2] "Understanding the Depth of the Global Ransomware Problem," An Osterman Research Survey Report sponsored by Malwarebytes, August 2016, https://www.malwarebytes.com/surveys/ransomware/?aliId=13242065

[3] David Fitzpatrick and Drew Griffin, "Cyber-Extortion Losses Skyrocket, Says FBI," CNN Tech, April 15, 2016, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

[4] Zack Whittaker, "Bought a Car Recently? Millions of Dealership Customer Details Found Online," ZDNet, Nov. 8, 2016, http://www.zdnet.com/article/bought-a-car-recently-millions-of-customers-records-found-online/

crowe.com

Text created in and current as of August 2017; Cover and artwork updated in May 2018.

RD-17000-026D