SEDONA SAFEGUARD

HOW TO DRIVE CYBERSECURITY EXCELLENCE ACROSS YOUR DEALERSHIP

THE DEFINITIVE GUIDE FOR DEALER PRINCIPALS

SEDONA SAFEGUARD

The Role of Dealer Principals in Ensuring Cybersecurity Excellence

In the wake of recent cyber-attacks on Snowflake, CDK Global, and AT&T, cybersecurity should be a paramount concern for all dealer principals. The potential financial, reputational, and operational business losses make it imperative for dealer executives to adopt proactive and comprehensive cybersecurity measures.

This executive guide discusses the role dealer principals play in safeguarding their businesses from cyber-attacks and threats. We offer insights, strategies, and best practices for effectively leading cybersecurity excellence across your dealership in partnership with your IT leaders and team.

Understanding the Difference: Compliance vs. Cybersecurity

Compliance and security often go hand-in-hand in the realm of cyber threat protection. Both aim to reduce risk, yet they are not mutually inclusive. Not everything required for compliance will enhance security, and not all security measures ensure compliance. It is crucial to understand how these two concepts interact and how they affect each other to stay ahead of threats.

What's the Difference?

Compliance refers to adhering to rules and regulations set forth by government, industry standards, or individual companies. These regulations aim to lower risk but have a broader scope than an organization's internal security measures. They focus on reducing legal, financial, and physical risks for organizations, employees, and customers. Compliance also requires proof to ensure conformity to these rules.

Security, on the other hand, is focused on preventing, detecting, and remediating cybersecurity incidents, such as cyber-attacks and data breaches. It involves protecting data in motion and at rest, at endpoints, and wherever it is stored, while maintaining measures to monitor activity and detect potential incidents. **The subtle yet critical difference is that security aims to protect the organization's assets, whereas compliance ensures adherence to policies.**

SEDONA SAFEGUARD

The Role of Dealer Principals in Ensuring Cybersecurity Excellence

How Compliance and Security Interact

While many aspects between compliance and security overlap, conflicts can arise. There are instances where compliance and security are at odds. Organizations may lack the resources to appoint dedicated compliance police, and proving compliance can distract from broader more impactful cybersecurity efforts. Compliance regulations, such as privacy rights, can complicate monitoring suspicious behavior. Additionally, documenting compliance can be laborous, especially if done manually.

Governmental regulations like California's CCPA or the EU's GDPR are designed to protect against cyber threats and privacy violations. Compliance with these regulations is often required for conducting business in specific regions. As regulations vary globally, organizations must stay current with multiple regulatory entities to maintain operations and reach potential customers.

The Key Is Striking the Perfect Balance

Despite the challenges, organizations can find a balance between compliance and security. Implementing measures for compliance can also improve security posture. For example, increased focus on visibility helps both security and compliance by making documentation easier and saving time for compliance teams.

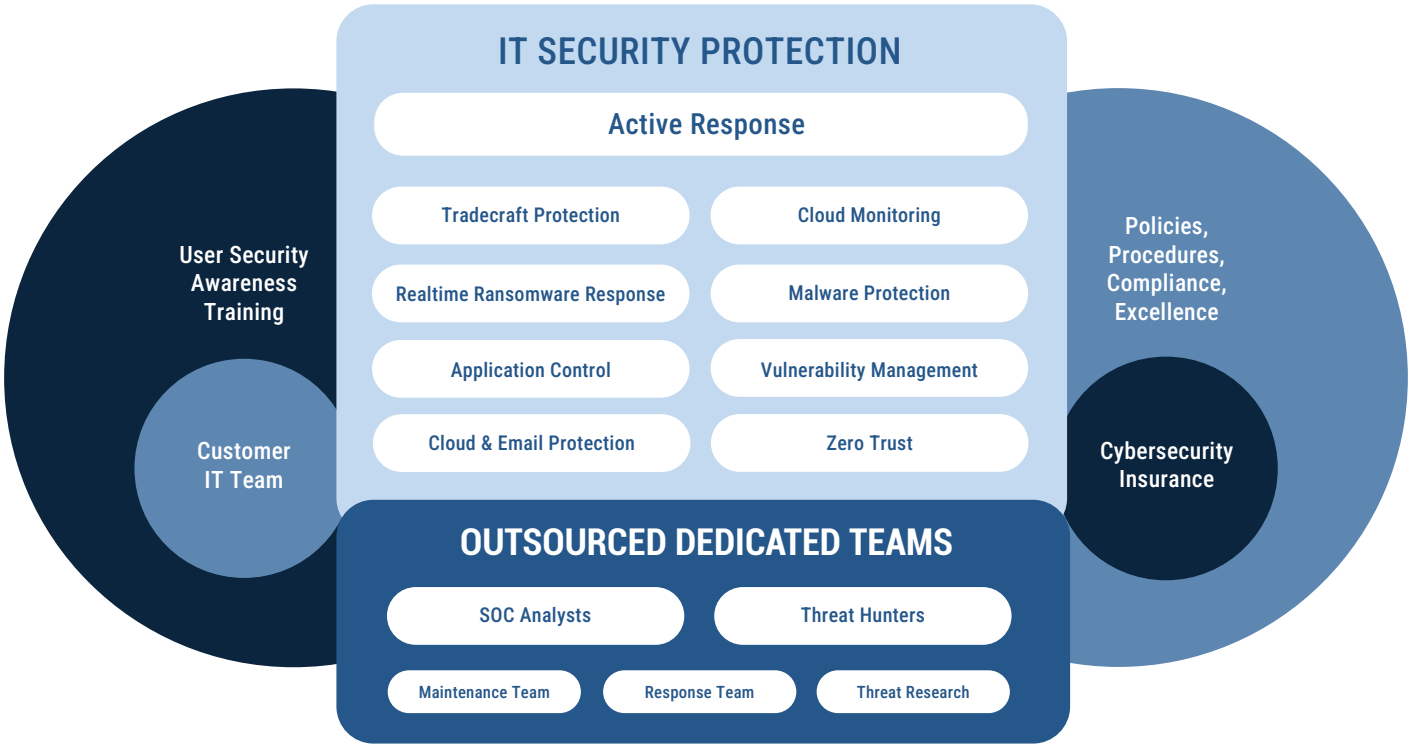
Regulatory measures, such as firewalls, incident reporting, and solutions to mitigate ransomware and phishing, lower risk and improve security. Thus, by adhering to compliance regulations, organizations also enhance their security.

SEDONA SAFEGUARD

Managing Cybersecurity with Excellence

Based upon decades of managing technology for dealers, we have developed a comprehensive framework by which dealers should manage their IT security. We call it. “The Ideal Comprehensive Cybersecurity Strategy.”

THE IDEAL COMPREHENSIVE CYBERSECURITY STRATEGY



This strategy is not a checklist for compliance but a holistic approach to managing cybersecurity. The goal of cybersecurity excellence is to deliver the best business, technology, and processes to minimize as many IT threats and security challenges as possible in a cost-effective manner.

The question you need to ask yourself as a dealer principal is simple:
How close is your current state of cybersecurity to this ideal?

SEDONA SAFEGUARD

3 Key Considerations for Dealer Principals Regarding Cybersecurity

1. Your IT Team Will Never Be Enough

Cybersecurity is an ongoing arms race. Threat actors are increasingly sophisticated, using AI to scale their attacks. There will always be vulnerabilities, ransomware, and gaps in your IT security stance. Dealer principals must accept that cybersecurity is a continuous challenge with constantly moving goalposts.

2. Outsourced Partners Are Experts

Your external cybersecurity partners are experts because they see more—more solutions, user security challenges, devices, threats, and threat actors. This broader perspective enables them to manage, detect, and respond to risks and threats more effectively. Encourage your IT leaders to leverage these external experts to enhance your cybersecurity strategy.

3. Your Employees Are Part Of The Problem

Researchers from Stanford University found that approximately 88 percent of all data breaches are caused by an employee mistake. This includes not only your employees but also those of your vendors and supply chain partners. Addressing this requires leadership from both IT and executive levels. Promote best practices, reward cybersecurity excellence, and incorporate security awareness training into all employee training activities.

While there are likely other considerations in your dealership, we find that these 3 are universal challenges for dealers.

SEDONA SAFEGUARD

The Role of Dealer Principals in Driving Cybersecurity Excellence

Dealer principals must adopt a proactive approach to managing cybersecurity, recognizing its broad impact on financial, reputational, and operational aspects of the business. This is not just an IT problem but a business problem, making it a leadership challenge.

Financial Considerations

Typically, IT investments are evaluated through "Total Cost of Ownership" analyses. However, cybersecurity should be assessed based on "cost of incremental risk management." Dealer principals need to quantify the incremental investment required to enhance protection and determine if it is worth the cost to mitigate the risk.

Operational Considerations

Many dealers trust their technology vendors to have the best security in place, but this is not always the case. Vendors are incentivized to sell more solutions, not necessarily to prioritize cybersecurity. Dealer principals must ensure that technology partners adhere to ideal cybersecurity strategies and incorporate risk analysis into the business system selection process.

Reputational Considerations

As an example, The CDK Global breach also caused significant reputational damage, with approximately 56,200 vehicle sales lost. This figure does not include damages to consumers, litigation costs, and other related expenses. Affected dealers upset a large number of customers by not adequately protecting their business systems.

CASE EXAMPLE: AUTONATION & THE CDK BREACH

The CDK Global's breach resulted in significant financial losses for AutoNation. According to their SEC filing, they saw a profit reduction of about $1.50 per share. This translates to over $60 million in lost profit. Had AutoNation, Invested a fraction of this amount in better cybersecurity, backup, and recovery solutions they could have prevented such losses.

LET OUR CYBERSECURITY INSURANCE PROGRAM LOWER THE COST OF RISK MANAGEMENT

THE KEY BENEFITS OF SEDONA SAFEGUARD INSURANCE PROGRAMS

- **Save up to 30% of Your Annual Insurance Premium** — We collaborate with you to reduce your insurance premium through our True MDR product.
- **Add Cybersecuirty Warranty** — Our Cybersecurity Warranty Program is a cost-effective way to lower your insurance costs, but raising your dedecutible, but still be protected.
- **Insurance Support Program** — We can partner with your finance, operations and legal teams to make sure that you are getting the most return from your cyberliability insurance and we can help you complete those pesky forms.

CYBERSECURITY INSURANCE WARRANTY PROGRAM CASE STUDY

Primary Cybersecurity Insurance - $2 Million Policy	Increased Deductible to $25k / year, Reduced premium by $3250 / year
Supplemental Cybersecurity Warranty Cost	$1920 / year
Insurance Savings	$1330 / year

SEDONA SAFEGUARD

Key Takeaways for Dealer Principals

Be Strategic About Cybersecurity

View cybersecurity as an investment, not just a cost. It requires an executive champion who can articulate a vision for security, implement change, and galvanize cross-departmental collaboration for success.

Champion Better Cybersecurity

- **For Your IT Team:** Highlight the importance of cybersecurity at the executive level in terms of financial risk and business protection.
- **For Your Employees:** Integrate cybersecurity awareness training into all business training, including onboarding for new employees.
- **For Your Company:** Develop well-thought-out policies, procedures, and partner selection processes to mitigate long-term cybersecurity risks.

Think Proactively Not Reactively

Cybersecurity must be a proactive initiative led by dealer principals. Include cyber education in your business education to stay informed about current IT security issues. Collaborate with cybersecurity partners and your CIO to educate your leadership team on best practices and strategies.

Conclusion: Fostering A Culture of Security

Dealer principals need to foster a company-wide culture of security. This cultural change must start from the top, with leaders demonstrating a commitment to cybersecurity excellence. By doing so, dealerships can better protect themselves from the growing threat of cyber-attacks and ensure long-term business success.

SEDONA SAFEGUARD

Sedona Safeguard Ensuring Compliance & Security

John Deere dealers, along with other heavy machinery dealers, must adhere to specific compliance standards like the Dealer Security Compliance Framework (DSCF) and the FTC Safeguards Rule. These standards are designed to protect consumer information and ensure secure operations within the dealership.

For example, The DSCF, developed by John Deere, consists of a comprehensive set of controls that align with some of the controls found in the CIS v.8.1 security standards. These controls cover areas such as data encryption, regular security assessments, incident response planning, and employee training, ensuring that dealerships not only comply with regulations but also enhance their overall security posture.

Similarly, the FTC Safeguards Rule mandates that dealers develop, implement, and maintain a comprehensive information security program to protect customer information. This includes appointing a designated security coordinator, conducting risk assessments, implementing safeguards to control identified risks, and regularly testing the effectiveness of these safeguards (bus64-ftcs-privacy-rule…).

Sedona Safeguard is an ideal solution for dealerships seeking to meet both cybersecurity and compliance requirements. Our solution integrates advanced threat detection, real-time monitoring, and comprehensive incident response capabilities with compliance management features. By adopting Sedona Safeguard, dealerships can ensure they meet DSCF and FTC Safeguards Rule standards while also enhancing their overall cybersecurity posture.

VISIT: WWW.SEDONASAFEGUARD.COM

OR CALL: (877) 854-3548