



THE DEALER CYBER SOLUTIONS TIMES

Microsoft
Partner

Silver Cloud Platform
Silver Cloud Productivity
Silver Small and Midmarket Cloud Solutions

DID YOU KNOW?

Our Blog is filled with helpful technology tips and insights for your business. We post new articles that provide valuable information for your business almost every day. You can sign-up to be notified of new topics when they are posted or you can visit <https://www.dealerCybersolutions.com/blog/>

Here are a few examples of the kind of information that is available:

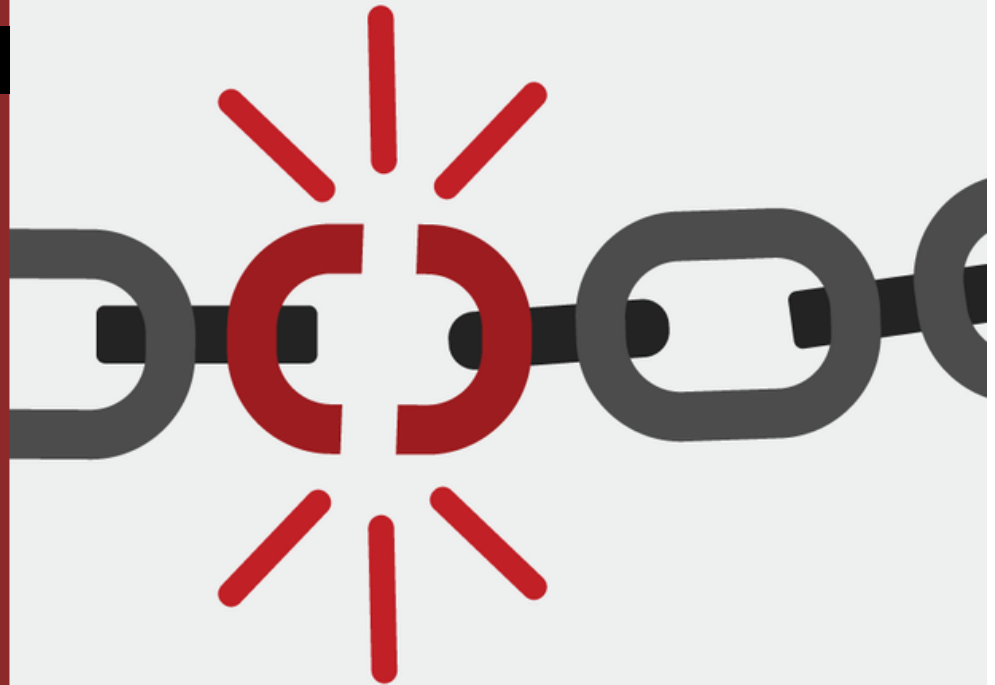
- The Role of IoT (Internet of Things) in Enhancing Dealership Operations:
<https://www.dealerCybersolutions.com/role-of-iot/>
- The Importance of Security Awareness for Employees:
<https://www.dealerCybersolutions.com/using-da/>

This monthly publication is provided by Dealer Cyber Solutions



OUR MISSION:

"As a dealership owner or leader, you don't have time to waste on worrying about cybersecurity threats and compliance requirements. That's our expertise. Call us and we get you on the right track so can stay focused on what's important- growing your dealership."



THE WEAKEST LINK: WHAT SUPPLY CHAIN ATTACKS MEAN FOR YOUR DEALERSHIP

Supply chain disruption is nothing new. We have all been impacted by a supply chain disruption at one time or another. Caused by production delays, natural disasters, or suppliers going out of business, you have been faced with the dreaded "out of stock" message at some point. You were able to move past the disruption with relative ease and likely never looked back.

You and your dealership are now facing a new breed of supply chain disruption referred to as a "supply chain attack" and this type of event will have immediate and lasting impacts to your business and your bottom line. You may likely have been a victim of the CDK Global cyber-attack and had your sales, finance, and service

operations forced offline and had to resort to old school pen and paper processing for weeks.

Breaking Down A Supply Chain Attack

A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. By compromising a single supplier, attackers can gain access to numerous downstream companies and their clients. This amplification effect allows cybercriminals to maximize their impact and potential gains from a single point of entry. As many dealerships rely heavily on their

continued on page 2...

...continued from cover

supply chains for essential services and products, disrupting these can cause significant operational and financial damage, making the targets lucrative.

The bottom line is that your suppliers often have access to your critical systems and sensitive information of your clients. Compromising your supplier can provide attackers with access to this valuable data.

The Impact Of A Supply Chain Attack:

- 1. Operational Disruption:** A supply chain attack could lead to system downtimes, and significantly disrupting your daily operations.
- 2. Targeting Your Dealership:** Within the 1st day of the CDK Global cyber-attack, cybercriminals were sending emails and making phone calls to dealership employees posing as CDK Global staff. Their intent was to prey on the heightened emotions of staff by masquerading as a helpful CDK Global employees. They were able to gain further access into dealership systems using these techniques.
- 3. Data Breach:** Sensitive customer information such as names, contact details, financial information, and social security numbers could be compromised. This exposure can lead to identity theft and financial fraud. Also, your proprietary business information, including sales data, pricing strategies, and financial records, could be exposed, putting

your dealership at a competitive disadvantage.

4. Financial Costs: There are immediate costs associated with identifying, containing, and mitigating the breach.

5. Long-term Financial Losses: Your dealership may face potential compensation claims from customers affected by the breach. Also, don't minimize the impact of the loss of customer trust that can lead to a decline in sales and long-term damage to your brand.

6. Compliance Violations: Dealerships now must comply with the Safeguards Act. A data breach could result in significant fines and sanctions to you from regulatory authorities.

How To Limit Your Exposure To A Supply Chain Attack

There is no question that your dealership is dependent upon 3rd party suppliers. You may also feel like you have little to no control over their security practices. To some extent, this may be true but here are some things you can do to prevent becoming a victim or minimize the impact of a supply chain attack.

- 1. Vendor Management:** Reassessing the security practices of all third-party vendors and partners to ensure they adhere to robust cybersecurity standards.
- 2. Contractual Safeguards:** Including specific security requirements and breach notification clauses in contracts with your suppliers.

3. Strengthening Your Security Posture:

Invest in stronger cybersecurity measures, including advanced threat detection systems, regular security audits, and employee training programs.

4. Incident Response Planning: Develop and regularly update incident response plans to quickly and effectively handle future breaches.

The above items can be overwhelming especially when you have enough on your plate just trying to focus on your day-to-day business operations. This is where Dealer Cyber Solutions can help. As a specialized cyber security company with over 25 years in business, we have the cyber security network engineering staff expertise to help navigate this cyber security threat your dealership is facing. We have the tools and real-world knowledge working with dealerships to assess the security practices of your suppliers, strengthen your cyber security posture, and deliver an incident response plan should you face a supply chain attack.

One thing is for sure, the time to act is now before you unwillingly become a victim of a supply chain attack. Let's start the discussion today- contact us at 810-354-1092 or visit: <https://www.dealerCybersolutions.com/>.

FREE Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Dealership Now

At no cost or obligation, our highly skilled team of IT pros will come to your dealership and conduct a comprehensive cyber security audit to uncover loopholes in your dealership's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the dealerships we've done this for discover they are completely exposed to various threats in a number of areas.

To Get Started And Claim Your FREE Assessment Now, Visit: <https://www.dealerCybersolutions.com/analysis>



CARTOON OF THE MONTH



DONALD MILLER

EXPLAINS HOW TO TALK ABOUT YOUR BUSINESS SO CUSTOMERS WILL LISTEN



It's really, really hard to grab people's attention today. Customers are busy and inundated with choices, making it hard for businesses to stand out. Donald Miller empathizes. He knew people loved his book *Building A StoryBrand* – after all, he sold millions of copies. But when Miller decided to tour and fill 700 theater seats for a speaking engagement, half remained empty. “I learned that I’m good at writing the 300 pages but not very good at writing the sentence that makes you want to read the 300 pages. It’s two different skill sets,” Miller explained to business leaders at a recent industry conference.

Do you know how to communicate the value of your products or services so customers buy again and again? Most of us don't. That's because we prioritize creativity and cleverness over clarity. Miller argues that no dollar spent on branding, color palettes, logos or website redesigns will help if you aren't clear about your message. Why? Because human brains are hardwired for two things:

1 Survive And Thrive

2 Conserve Calories

We don't have time or energy to process unnecessary information; we only buy what helps us get ahead. “If you confuse people about how you can help them survive, you'll lose,” Miller says.

Tell A Story

“The first thing we have to understand is that people buy products only after reading words or hearing words that make them want to bother to buy those products,” Miller explains.

Let's say you meet two people at a cocktail party

who do the same thing for a living. You ask person A, “What do you do?” They say, “I’m an at-home chef.” So, you ask questions about where they went to school, their favorite recipes, etc. Then, you meet person B and ask the same thing. They respond, “You know how most families don't eat together anymore? And when they do, they don't eat healthy? I’m an at-home chef.”

Who does more business? Person B, because they told a story about how they solved a problem. Humans love stories; it's why we binge-watch good television. Good stories have the same core structure, and Miller explains how you can use it to tell the story of why your business is the one customers should choose.

Identify your hero's (customer's) problem and talk about it a lot. When someone asks, “What do you do?” don't tell them. Start by describing the problem. Spend 75% of your time talking about your customer's problem because that triggers the purchase.

Introduce them to the guide (you). The key to being a guide is to listen: “I’m sorry you're going through that. It sounds very stressful.” Then, be competent: “I feel your pain, and I know how to get you out of this hole.”

Give them a plan. This is an active call to action, like “Buy now” or “Schedule a call.” You must challenge the hero to take the action that leads to success.

Remember, the story you're telling is not about you. It's about your customer, the hero. Once you have your message, distill it into short, simple and repeatable sound bites. “It works every single time,” Miller says, “because the human brain cannot ignore a story.”

SHINY NEW GADGET OF THE MONTH

Pocket Projector

Take movie night to your backyard, park, campsite or wherever adventure takes you. The ELEPHAS 2024 Mini Projector offers impressive features in a compact, smartphone-sized device at an affordable price. The projector has 1080p HD resolution for clear and detailed images, uses a heat dissipation system to reduce fan noise and has a built-in hi-fi speaker that offers excellent sound quality without external speakers. It also includes USB, HDMI and AV ports and is compatible with laptops, PCs, TV boxes and smartphones. You can even connect it directly to your Amazon Fire Stick or Roku Streaming Stick.

With a carry bag and mini tripod, the ELEPHAS Mini Projector is high-quality, portable viewing so you can take family movie night anywhere.





INSIDE THIS ISSUE

The Weakest Link: What Supply Chain Attacks Mean For Your Dealership P. 1

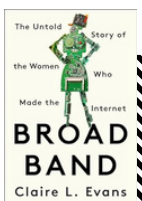
Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Dealership Now P. 2

Donald Miller Explains How To Talk About Your Business So Customers Will Listen P. 3

BROAD BAND

By Claire L. Evans

In tech, there are stories we hear all too often: a major company got hacked, Meta dealing with yet another lawsuit or Google implementing some new security measure. However, there's one story we don't hear enough: pioneering women in tech. Much like *Hidden Figures* and *Rise of the Rocket Girls*, *Broad Band* by Claire L. Evans uncovers the pivotal yet overlooked contributions of female pioneers who shaped the Internet.



Evans vividly narrates the achievements of visionaries like Grace Hopper and Elizabeth "Jake" Feinler, showcasing their revolutionary work in computing and online networks. Evans sheds light on these hidden figures, inspiring a new generation to recognize and celebrate the women behind technological advancements. *Broad Band* is an essential, enlightening read that helps redefine the true history of technology.

VPNS ARE NOT AN INVISIBILITY CLOAK

(Don't Use Them Like One)

A virtual private network (VPN) is essential for modern office work to create a secure, encrypted connection between your device and a remote server, allowing you to work from anywhere while protecting sensitive data. VPNs are also gaining popularity for personal browsing by routing Internet traffic through a remote server to mask your IP address. It's like a gated tunnel only you can enter, which is handy for accessing region-restricted streaming services or content and protecting data when using public WiFi.

However, some people confuse VPNs with an invisibility cloak, believing that anything they do online while using a VPN is hidden. That is not the case. Some VPN services log your data (which can be leaked, hacked or sold), and there are other ways cybercriminals can track you online. Understand what VPNs do and don't do so you aren't putting yourself at unnecessary risk.

What VPNs Do (And Don't Do)

VPNs are excellent for enhancing privacy and security. **They DO:**



Hide your IP address, making it harder for websites and advertisers to track your online activities.



Encrypt your Internet traffic, safeguarding sensitive information like passwords and business communications.



Allow access to geo-restricted content, which can be beneficial for business research or accessing region-specific services.

Despite these advantages, VPNs have limitations. **They DON'T:**



Make you completely anonymous. While your IP address is hidden, websites can still track you using cookies and other tracking methods.



Protect you from malware or phishing attacks. A VPN cannot filter malicious content, so you still need robust antivirus software and cyber security practices.



Prevent all data logging. Some VPN providers may log your data, so choose one with a strict no-logs policy.

Warning: Avoid Free VPNs!

Free VPNs are dangerous. Many free services log your data and sell it, undermining the very privacy you're trying to protect. Free VPNs may also have weaker encryption standards, exposing you to more risks. Always opt for reputable VPN providers with clear privacy policies and transparency about how they use your information.

How To Use A VPN Responsibly

- **Choose A Reputable Provider:** Look for VPN services with strong privacy policies, good reviews and transparency about their data-handling practices.
- **Enable Kill Switch:** This feature ensures your Internet connection is severed if the VPN connection drops, so your data won't be leaked.
- **Update Regularly:** Keep your VPN software updated to benefit from the latest security improvements.
- **Combine With Other Security Steps:** To maximize protection, use a VPN with antivirus software, firewalls and good cyber security hygiene.

Understanding VPN capabilities and limitations ensures you use them effectively and responsibly, protecting your data without relying on a false sense of invisibility.

DON'T FORGET TO CHANGE NEW-HIRE PASSWORDS

To keep things simple, employers often create easy, temporary passwords for new hires to log in to accounts or devices during their first few days. However, a Specops analysis of millions of passwords found that 120,000 used common words related to new employees, meaning the new-hire passwords were never changed. Hackers know this and use these simple password structures in brute force attacks. The most commonly compromised

passwords on new accounts are user, temp, welcome, change, guest, starter, logon and onboard. Look familiar? Prevent this mistake by forcing change at log-in (if possible), using a service like First Day Password or an authenticator app or making a new-hire password REALLY hard.

