

Cybersecurity:

Safeguarding Your Business in the Digital Age



WennSoft

Proven Solutions. Lasting Relationships.

Introduction

The digitization of our society has had a powerful impact on the ways in which organizations work and relate to their customers and each other. Whether it be social networking or mobility or the acceptance of “always on, always connected,” we live in a hyper-connected world. Sadly, within all of the positive outcomes of these powerful relationships, lurks evil: a sophisticated and organized “cyber underground” with one goal – to exploit all these connections for financial gain. Who could have imagined just a few years ago that data security would be one of the key risks facing field service organizations?

For businesses that hold vast amounts of customer data, and are moving their mobile work forces to a digital environment, questions arise fast and furious. How do we protect ourselves? What are the risks? What can I do to address these challenges before something happens?

This ebook explores the data security challenges of the digital age and the questions that field service leaders should be asking themselves and their organization to help keep their systems, their data and that of their customers secure.

Table of Contents

Introduction	2
Chapter 1 – The Great Target Data Breach...Why It Hits Home	4
Chapter 2 – 7 Tactics to Mitigate Risk and Reduce Liability	7
Chapter 3 – Eight Isn't Enough: Upping Your Password Ante	10
Chapter 4 – Cash or Credit? Secure it!	14
Chapter 5 – And (as if that wasn't enough) Here Comes BYOD.....	16
Final Thoughts	19

CHAPTER 1

The Great Target Data Breach...Why It Hits Home

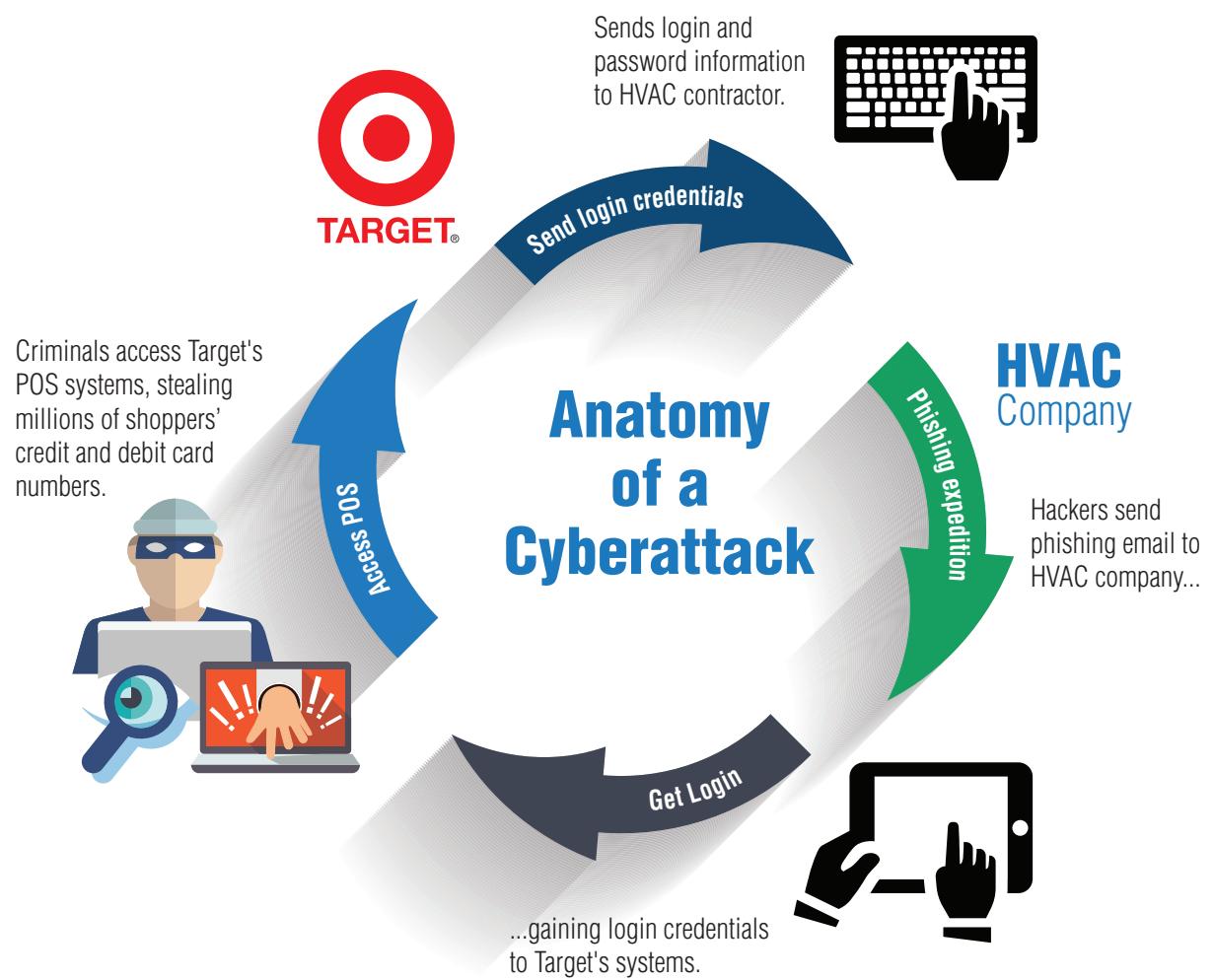
In December 2013, Target® announced that it had become the victim of a cyberattack that ultimately resulted in the theft of more than 40 million credit and debit card numbers and the records of more than 70 million Target shoppers. The Target breach wasn't the first attack to hit a large, well-known business, nor will it be the last. Similar attacks have taken place at Neiman Marcus®, Michaels® and still more recently, at SONY®.

The Target breach hits close to home for many service companies because the hackers reportedly accessed the Target systems through a mechanicals contractor that did work for the retailer.

What Happened...

As is often a customary practice between business partners, Target allowed its contractors to access their system so they could enter their bills for payments and information about what they completed on work orders.

Through a phishing attack at the HVAC company, the hackers found an email from Target issuing a contractor network login credentials, information that included a username, password and directions on how to access Target's system.



And How...

Two specific business practices made it easier for the hackers to access Target's system.

First, on Target's end, the retailer put an enormous amount of information on their external website to publicly inform vendors who wish to do business with them how they would access their system. Doing so essentially gave the hackers a map of how to break into their system.

Second, while the mechanical contractor was using anti-malware software, they were using a free version that was designed explicitly for individual PC users, not for businesses. Also, the software worked as an on-demand scanner and didn't automatically check for new threats; unless someone in IT initiated a scan, it sat idle.

Those two weaknesses are among several areas that you as a field service leader should examine to ensure you're doing everything you can to protect your business and your customers. Unfortunately, there is no perfect way to protect yourself from all criminal activity.

The key is to limit your risk and liability as much as possible. And it's all about answering the question: How do you as a contractor keep from holding the bag for something that goes wrong?



How do you as a contractor keep from holding the bag for something that goes wrong? It's all about limiting your risk.



[Flip to Chapter 2 for some answers.](#)

CHAPTER 2

7 Tactics to Mitigate Risk and Reduce Liability

Tip: When talking to your employees, don't start with horror stories about the bad things that could potentially happen due to lax protocols. The minute they start feeling like there's some threat or they may be doing things wrong, they will likely clam up out of fear, and you won't be able to get the information from them that you need.

Do you know where your customer information is? If you answer "no," "sort of," or "I think so," you've got some work to do. Even if you answer with a vehement "Yes!" it probably won't hurt to revisit how you're protecting customer information, especially if it's been awhile since you set your policies.

When it comes to safeguarding your business from a security breach, there is no solution that offers 100 percent protection. But there are some things you can do to mitigate risk and reduce liability.

1. **Review your organization's procedures.**

Start by sending all your employees a simple questionnaire that includes questions like: Do you work with credit cards? Do you log into customer systems? Do you manage any customer information that has to do with credit cards or numbers for their systems?

Once you've identified who has access to what data, meet with those people to understand what they're doing. Ask lots of questions. Update or establish procedures for safeguarding the sensitive data.

2. Ensure your software is legitimate.

If you manage your email and firewall systems, make sure you're using software that you are legally licensed to use, and that is designed for use by a corporation. According to reports, the software used by the contractor linked to the Target breach was a free version of an anti-malware program designed for personal use, requiring manual updates and human intervention. With a more robust program, the breach may never have happened or may have been caught at a much earlier stage.

3. Hire a company to test your security.

There are a number of organizations out there that specialize in breaking into business systems to test their security. Hire them to hack you. Chances are, they will and in the process can pinpoint the areas where you need to up your protection. While it may cost several thousand dollars to hire such a company, an ounce of cyber protection could save you pounds in headaches and litigation costs if your data is compromised.

4. Consider the cloud.

Think about using an outside provider to host your systems in the cloud. Cloud or SaaS vendors provide all the security and network coverage you need and have built-in backups so your system won't go down. Be sure to review your terms of service with the provider to ensure that your company's information and activities (and those of your customers, if relevant) are protected.



5. **Create a passwords policy.**

You need to have a written policy on passwords and make sure people understand that policy.

Consider having your employees sign a confidentiality statement stating that passwords and access to systems are for their use only. [For tips on passwords, see Chapter 3 When Eight Isn't Enough: Upping Your Password Ante.](#)



6. **Protect credit card information.**

These days, more and more people are paying with credit cards so they can earn points. If you don't take credit cards today, demand may require you to in the future. You must have written policies in place that spell out which pieces of customer credit card information should be stored and which shouldn't, and that describe exactly where and how that information should be stored. [See Chapter 4 Cash or Credit? Secure it!](#) for more tips.

7. **Get insurance.**

In this digital world, when a criminal breaks into your network and causes damage to somebody you're connected to, the typical liability policy will not cover that claim. Make sure you have insurance to cover you and your customers in the event of a criminal attack. You want your coverage to provide for private and corporate confidential information – all of it – not just credit cards and social security numbers, but ALL private information. Online and offline. And “offline” includes the dumpster outside because if private information ends up in it and is stolen, you've just had a breach.

CHAPTER 3

When Eight Isn't Enough: Upping Your Password Ante

According to a 2014 survey by the Ponemon Institute, 71 percent of employees report that they have access to data they should not see, and more than half say that this access is frequent or very frequent.



Contractors are in an especially sensitive position because they often deal with passwords for not only their systems, but also those of their customers. If your employees have access to customer systems, how do you safeguard the password and login information that your employees use? After all, it was a phishing email at a vendor's business that caused one of the largest data security breaches in US history.

How many of you have gone into a building owner's building automation system, opened the panel, and seen logins, passwords and dates written in magic marker on the inside of the door? Sure that makes it easy for any technician to come in and know what the login and password are. And that's the problem: anyone walking into that building can open the panel, and they essentially have the keys they need to access the system. Sound ludicrous? It happens. It might be happening to you.

Here are some guidelines to consider when evaluating your procedures for password safekeeping.

The 5 Principles of Password Protection

1. **Passwords Must Be Handled with Care**

Where your employees store passwords and login information and how they safeguard them are important factors for keeping data secure.

How many of you include the login information when you print out a work order for your technicians or send it out electronically? When your technicians get done with the job, they probably make a copy of it and hand it to the customer to keep. The person they hand it to might be the maintenance guy, who may or may not need to know the password to get into the system. The maintenance guy may pass it to an admin, who gives it to someone else in billing, and now three people have the password who probably don't have any need to know it. Bottom line, your employees shouldn't be giving their password to anyone, even someone at the company they're doing work for.



2. **Passwords are Not Meant for Sharing**

If your employees share passwords with their fellow workers, and one of those workers leaves, you might not be aware that he has the password and login information for one or more customers. That former employee could start working for a competitor and could try to use that password to access the customer's system again. Guess what? The password still works, because nobody knew he had it. Prevent that from happening by making it a policy that employees should not be sharing passwords.

3. **Passwords Need to Be Changed**

Changing passwords on a routine basis, like every quarter, takes some work. But it takes a whole lot less work to change a password than it does to figure out when and how somebody accessed something that they weren't supposed to. By requiring routine password resets every quarter, at least every three months you know everyone's got new passwords, and the old passwords, that someone might have gotten when they shouldn't have, won't work anymore.



4. Passwords Must Be Strong

Authentication methods, that require additional evidence to prove you are who you claim, are safer than a static password. If possible and practical, use them. Your policies should also allow employees to use strong passwords without tempting them to reuse passwords or write them down so they can remember them.

5. Password Security Must Reach Beyond Your Business

Passwords given to your customers to access systems that you provide also need to be protected. If one of your customer's password-holding employees leaves, do they notify you? If they don't tell you, and give you the opportunity to reset that password that employee could go somewhere else and still access the system. But even if you ask your customers to notify you when an employee leaves, there's no guarantee they're going to do it.

The important thing is that you have that policy in writing, and you've made them aware of it. You have essentially provided them with a way to protect themselves, and if they choose not to do it, it's on them. Having a written policy that customers need to notify you when an employee leaves reduces your liability.

CHAPTER 4

Cash or Credit? Secure it!

A staggering 43% of companies have experienced a data breach in the past year.

– PONEMON INSTITUTE

Taking credit card payments online provides a convenient way for your customers to pay their bills. However, it also opens a door for a number of security risks.



If you don't use software to collect credit card payment information, and instead have created a form on your website for customers to enter their information, you are likely in violation of quite a few requirements and laws geared toward accepting and processing credit cards. We see a lot of organizations with talented IT staff who, in an effort to help their organizations do business online and collect payments faster, create web pages to take credit card payments.

However, if your company doesn't encrypt credit card numbers, eliminate the security code after the transaction is processed, and hide the name and address from being associated with the credit card number, you are in violation of many of the credit card security requirements out there today. Even if you only take credit card payments over the phone, if you don't use software to take care of all the information gathered, you are picking up a great deal of risk and may be breaking your agreement with your credit card providers to take credit cards from customers.

Some customers may ask you to keep all of their information, so they don't have to call in and give you their security number each time. Security numbers are the keys to using a credit card number anywhere in the world. If you agree to keep that information on file, ask for a signed statement from those customers. The statement should state that the customer acknowledges that having your company store their information in that way is not as safe as if they gave it to you each time.

You should also think about who in your organization has access to credit card and security numbers. Not too long ago, I was walking through a customer's office and happened to glance into the cube of an employee who handled billing. Tacked to the back of the cube was a spreadsheet containing the company names, credit card numbers and security codes for their customers.

How easy would it be for anyone to walk by, take a picture of that spreadsheet, and sell all those credit card numbers and information to someone? I challenge you to walk back into any department at your business that takes credit cards, and find out where they store the credit card information and how many people have access to it. I think what you find out will be frightening.

If you take credit cards, you have to comply with the security standards set up by the Payment Card Industry Security Standards Council (PCI SSC). A couple of the standards include: requiring each customer has a unique password to use in the system, making sure you encrypt the data, and ensuring that you never, ever keep the security number for the credit card in your electronic system.

For more information on the PCI SSC standards, visit www.pcisecuritystandards.org/security_standards.

CHAPTER 5

And (as if that wasn't enough) Here Comes BYOD

Mobile devices have completely changed the field service business. So much work can be done quicker, faster, and better on a smart phone or tablet. When you think about it, field service technicians ARE the ultimate mobile workforce – no office and no landline required or (quite often) available.



However, the BYOD movement brings with it an additional set of security and data concerns. In the world of BYOB, the user commonly owns, maintains and supports the device, so you have significantly less control than if it was corporately owned and deployed. Multiply that one device by the number of employees that want this flexibility, and you've got a large number and a wide range of devices to consider. But saying NO to BYOD, means saying NO the bounty of goodness that comes with the mobile movement. Better to be prepared. Revisit your policies and procedures and establish secure options for mobile devices.

BYOD Considerations:

- What data is being captured and where will it be stored
- How data will be transferred (XML, PDF attachments, other) and whether there is potential for leakage
- How data will be cleared from the device if the employee leaves or is terminated
- How you will support user-owned devices and manage loss or theft

Top 10 Tips to Support B-Y-O-D Without Losing Your C-O-O-L:

1. Ensure you have an acceptable Use Policy in place (for all departments and all employees) to provide guidance and accountability of behavior. Review and sign annually.
2. Be specific about the types of personal data that can be processed on personal devices.
3. Register all devices with a remote locate and wipe service to ensure confidentiality in case the device is lost or stolen.
4. Have a process for quickly and effectively revoking access a device or a user might have in the event of loss or theft.
5. Provide user guidance on the risks of downloading untrusted or unverified apps or responding to phishing emails.
6. As with any device – user owned or corporate issued – insist on strong passwords.
7. Ensure device access is locked, or data automatically deleted if an incorrect password is attempted too many times.
8. Use encryption to securely store data on the device.
9. Ensure that the device automatically locks if it's inactive for a period.
10. Clearly separate the business data from the owner's data by using different apps for business and personal use.

FINAL THOUGHTS

The digital age has revolutionized the way we communicate and access information. And how we do business. Unfortunately, it has also proven to be a fertile medium for those that are dishonest and unscrupulous. Those morally challenged individuals regularly use these modern connections to steal personal information, much like the data breach that hit Target.

Let's face it, whenever you put information on a computer, that information becomes less secure. Connect that device to the Internet and the security risk compounds. But to conduct business, to compete, and to grow and profit in today's hyper-connected world, cybersecurity is a business investment "must have."

We hope these tips and considerations help you take a closer look at your procedures and policies to prepare better for this hyper-connected world and the cybersecurity demands that come with it.

But the learning doesn't have to stop here.

- Join the conversation (info.wennsoft.com)
- Visit www.wennsoft.com to learn more about field service solutions proven for the digital age.