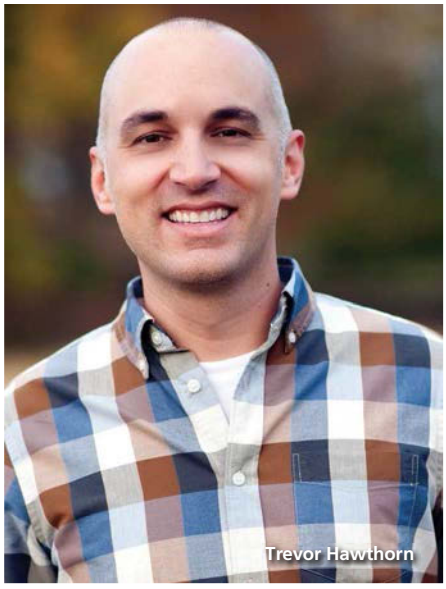
Protect and Secure

Technology alone won't stop security threats to retail

Trevor Hawthorn of Wombat Security Technologies has spent some 20 years as a maven of retail security. Based in Pittsburgh, Wombat provides information security awareness and training software to help organizations ingrain secure behavior in their workforces.

The Wombat chief technology officer has a unique take on security, including on the biting ramifications of cyber breaches for retailers and their customers. Hawthorn's words are both colorful and purposeful as he examines retail security from the inside out — from the back office to the point of sale. He is a former security assessor, qualified by the Payment Card Industry Security Standards Council, helping retailers comply with payments standards, and founded his own security firm.

Hawthorn believes that simply deploying the latest and greatest technology "is not a complete solution" to security. He says security is moving away from a singular focus on solely protecting systems by giving end users the training and tools they need to help stop attacks. This approach, Hawthorn says, is particularly vital for the retail industry, whose key operations often are in far-flung physical stores and distribution-center locations away from headquarters.


Trevor Hawthorn

Hawthorn discussed his ideas on retail security with STORES Contributing Editor M.V. Greene.

What is the retail landscape with regard to security and any concerns retailers should have going into 2017?

There are universal challenges that almost everybody faces. Everybody these days has data to protect. When it comes to retail, it is a little bit different. There aren't too many retailers left that have only a bricks-and-mortar presence. And even if they do, they're going to have some kind of electronic payment solution. Gone are the days of pure carbon-copy transactions.

Retailers also have a reputational risk to confront if something were to happen.

Certainly you suffer when it comes to the brand. Brands do tend to come back, but the cost comes from the interruption. It's the distraction. Whether you are a large or small retailer, responding to a breach — just having to deal with it — is no fun.

The problem is that as a retailer, depending on how your network is laid out, you now have this big, extended family of physical locations you have to protect. If you have wireless networks or computers in the back room that have a tie-in back into corporate, it just makes you a little bit more vulnerable.

On the one hand, there's an opportunity to do things more securely with technology, but on the other hand all of these things — like more advanced point-of-sale systems and loyalty programs and a mix of e-commerce and bricks-and-mortar — that's complex. One of the fundamental rules in security is complexity breeds insecurity. The more complex things are, the harder it is to secure. Like with a lot of things, it comes down to the implementation.

"There's a lot more technology that's required to run a retail organization now than ever before. As we've gotten away from carbon copies of credit card numbers and receipts just laying all over the place, it does give retailers the opportunity to do things in a more secure way."

— Trevor Hawthorn, Wombat Security Technologies

The retail industry has been the victim of a number of highly sophisticated cyberattacks in recent years. What's the posture of the cybercriminal these days? There seems to be no limit to the sophistication of their hacking efforts.

From the attackers' standpoint, whatever goods are easiest for them to monetize are what they will go after. If the credit card companies make it more difficult to use stolen credit cards, then that's going to make credit cards less attractive.

At the end of the day, it comes down to whatever can fetch the highest margin. It's kind of ironic: The bad guys are stealing cards or stealing identities or stealing database dumps of personally identifiable information, then they have to turn around and figure out what gives them the biggest margin. Some of the largest criminal groups have internal customer relationship management systems in place to see what their pipelines look like. You don't just steal credit cards and you're done. There's a whole process that you, as the bad guy, have to [undertake following] the credit card dump in order to sell the credit cards.

Whenever we talk about cybersecurity and breach, we think in the back of our heads about … these grand things where all our customer data just goes right out the door. But the other thing you have to think about is the straight-up interruption to your organization. That comes in two different forms. One is literally having to respond to it and calling someone in to help you to figure how bad it is.

The other one, that is making the headlines almost every day, is ransomware. Maybe you didn't lose any credit card data, but if you can't run a card during peak holiday season because of something like ransomware that mostly gets in because of malicious email attachments, that's something that would make for a pretty tough day.

How are retailers generally positioned for securing their operations in the face of these challenges, especially given that notoriously tight operating margins can crimp technology spending?

If you're a fast-growing retail organization that maybe doesn't have the full budget or expertise to build out advanced security capabilities, but you're growing so fast that you kind of need it, it creates a real challenge.

The good news is that in the last five to 10 years, we've seen a definite increase in retail security spend. I think PCI … has really driven retailers to make those investments. At the same time that retailers have driven security spending, there's also been the demands of the market to have nicer point-of-sale experiences for the customer or to have loyalty programs.

There's a lot more technology that's required to run a retail organization now than ever before. As we've gotten away from carbon copies of credit card numbers and receipts just laying all over the place, it does give retailers the opportunity to do things in a more secure way.

What are some impediments that retailers face on security? You have talked about a cybersecurity skills gap in organizations — can you

discuss that?

Retailers will say, 'We're a growing chain and we know that in order to act bigger than we are, we need to have this kind of [security] technology capability.' Then they will ask, 'Does anyone know how to properly implement it?' The answer within the organization is often no, but the customers want it now.

The [large retail chains] have enough money from a security standpoint that they can handle the technology spending and also hire the right people to implement their programs. But for most retailers, it's really tough to find the people that know how to implement the technology and to drive it.

Your company provides a software-as-a-service cybersecurity education solution with a tailored security training and awareness program for retail organizations, focusing on email security, social engineering, data protection and PCI training. How is your solution approaching the market?

Technology takes care of a lot of things, but it's not a complete solution. Every year there is new technology, and every new technology is cool. But one of the challenges everybody faces is that there are still phishing attacks exploiting end users.

> "We've seen a real renaissance in the user-awareness training space in the last several years. … I think organizations are starting to realize that you have to train end users."
>
> **— Trevor Hawthorn, Wombat Security Technologies**

That is still a very effective way to get to the retailer. How much time are the bad guys going to spend figuring out some exotic attack when they can just send an email to someone and get them to click? That's all it takes. Firewalls take care of a lot of things, but they don't solve everything.

We've seen a real renaissance in the user-awareness training space in the last several years. A lot of companies in our space have definitely grown because I think organizations are starting to realize that you have to train end users. There is still technology to be deployed, but you now have a much more user-oriented dynamic.

If you have someone with you for less than a year, or summer and seasonal workers, you don't have a week to put them through intensive security awareness training that maybe you have … for other people, such as with your corporate back-office folks.

From a retailer's standpoint, you have to figure out how to train a bunch of seasonal folks who are going to have access to credit card data, who are going to be keying information into cash registers or helping out in call centers. You have to have really succinct and bite-sized training modules to put them through, to give them a bit of a crash course. This is the most important thing you have to do today. STORES

M.V. Greene is an independent writer and editor based in Owings Mills, Md., who covers business, technology and retail.