BY KAREN EPPER HOFFMAN

ON ALERT

ONLINE RETAILERS ARE UNDER MOUNTING PRESSURE TO PROTECT THEMSELVES FROM CYBERCRIMINALS.

INTERNET RETAILERS ARE WAGING A two-front war. On one front, they face growing competition that's forcing them to shave costs and operate more efficiently. On the other, they're fending off cybercriminals who are using myriad tactics to eat into their profits and hamstring their businesses.

That's making life difficult for an online retailer like Find Me A Gift, which sells a wide range of gadgets, toys and personalized gifts, says Richard Grove, the retailer's information technology manager. "Small businesses [like Find Me A Gift] are increasingly coming under attack as hackers target smaller companies because they know many don't have the infrastructure or skills needed to fully secure themselves."

Successful and attempted cyberattacks in the online retail industry are growing. The number of cyberattacks that were identified and prevented in the third quarter of 2017 was double that of the same time period in 2015, according to digital identity firm ThreatMetrix's "2017 Q3 Cybercrime Report." And those are only the attacks the industry knows about, which many industry experts suggest may be just the tip of the cybercrime iceberg. As bad actors get better at plying their illegal trade, management consulting firm PwC has pointed to "financially motivated cybercrime [as] the biggest threat facing the retail sector" in its annual "Global State of Information Security Survey 2017" report. Retail companies suffered on average over 4,000 security incidents per year, with 16% of these businesses suffering losses of more than $1 million, PwC found.

MANY CRIMINALS ARE TARGETING ONLINE retailers because unlike many other high-profile businesses, such as banks, many merchants have not put as many resources or dollars into their cyber-defenses, says Zack Allen, manager of threat operations for cybersecurity firm ZeroFox.

"Social media has become a mainstay for these retailers and some of these accounts and pages yield millions of followers who are ready to click on links or follow advice," he says. "Cybercriminals use the benefit of social media and brand awareness as a way to 'poison the »

waterhole.'" Some criminals use social media to research and connect with consumers while others create fake websites or social media pages to draw in unsuspecting consumer victims.

Criminals are seeking to steal credit card and bank account information, personally identifiable information such as birth dates and Social Security numbers, as well as other customer and employee data. Their goal is to sell that information on the dark web, the online marketplaces where bad actors go to buy and sell personal data, malware and other exploits.

The threat to online retailers is growing because criminals are moving their game online as physical retailers—and their payment infrastructures—become more difficult to penetrate, says Christian Janoff, security solution architect at Cisco.

"Cybercrime is like a balloon. Squeeze one end and it bulges where there is the least resistance," Janoff says, adding that with the increasing adoption of chip cards that follow EMV standards in the United States, criminals have shifted their focus online. That's because chip cards and the EMV (short for EuroPay, MasterCard, Visa) standard are designed to make it more difficult for criminals to commit fraud in stores.

"Malicious actors like taking the path of least resistance," says Dan O'Sullivan, cyber resilience analyst for UpGuard's Cyber Risk team, an online security risk consultancy. "If one enterprise has some gaps in its armor but some decent security measures in place, and another has major weak points, malicious actors will focus their energies on the weaker target. Why waste your energy on a hardened target when there are easier victims to be had elsewhere?"

$1.3 MILLION

THE AVERAGE COST OF A DATA BREACH FOR LARGE COMPANIES

Source: Kaspersky Lab

IT'S NOT ONLY LARGE ONLINE merchants such as Amazon Inc., Apple Inc. and Walmart Inc. that draw the gaze of these online attackers. Some criminals target small and midsized online retailers that typically have fewer resources to fend off the onslaught.

Indeed, just over half (52%) of retail organizations consider their security infrastructure up-to-date and upgraded with the best technology tools, according to Cisco's "2017 Annual Cybersecurity Report."

"Bad actors aren't asking if [the retailer] is big or small, they're just looking for vulnerabilities," says Greg Schu, partner in advisory services for BDO, an accounting and consulting firm.

Those attacks come in myriad forms.

For instance, Find Me A Gift in the past year has seen a "huge" increase in the number of phishing emails directed at its employees, Grove says. Phishing attacks are efforts by criminals to make an email or website look like that of legitimate brand or sender to try to convince the recipient to click a malicious link or download a compromised attachment. Once an employee engages with the email, he may give the criminal unfettered access to the retailer's systems where the criminal can steal confidential information.

Combating emails requires "vigilance" on everybody's part, Grove says. That means retailers need to regularly review and update their employee rules and processes.

The weak point on most systems is its employees and while companies can do their best to educate their staff, they are still open to making mistakes. Unless retailers put up safeguards, such as developing an incident response plan and training all employees about the potential for attacks and what to look for, the threat will continue.

"Attackers tend to be lazy, they look for the low-hanging fruit and simple ways to monetize their attacks," says Larry Ponemon, chairman and founder of the Ponemon Institute, an information security research company. "They look at online retail and see it as a good place to attack because there are a lot of vulnerabilities in these organizations."

Some criminals target small and midsized retailers because those businesses often use "out-of-the-box" fraud tools that aren't tuned to their specific business and trends, says Michael Graff, senior fraud manager at technology vendor Radial.

These cyber-scams can include a blitz-attack of several small, quick malware deliveries or breaches over the course of a period of days to confuse and overwhelm the victim's business.

Others make a high volume of low-dollar orders to try and "trick" security or fraud tools, Graff says.

Both types of attacks can lead to an excessive chargeback warning from payment card companies that can impose fines as a result, or may even turn off the merchant's ability to accept payments on the site, he adds.

CYBERSECURITY CONCERNS CANNOT BE FIXED or mitigated until the retailer recognizes the problem. That requires retailers to embrace the idea that it is not a question of if it will be attacked, but when it will suffer a breach or attack, experts says.

"Online retailers need to acknowledge the risk fraud poses to their companies because even if they have not been hit in the past, chances are, they will be in the future in some way," Graff says. "While unfortunate, criminals are masters of technical ingenuity and are constantly developing new and unexpected ways to attack. With the size and complexity of the problem continuing to grow, it's critical that retailers understand the risk to their organizations, and that they properly assess whether or not the steps they've put in place will be sufficient enough to mitigate that risk."

While the cybersecurity problem may seem insurmountable, industry experts say online retailers must focus on changing what they can within their own organizations to make them more secure and fault-tolerant, and looking to how a breach could affect their business, the customers, and their reputation.

Online retailers' threat models need to be aware of how criminals view their brand's security, says Sam Curcuruto, head of product marketing at RiskIQ, a company that offers cloud-based malware and phishing detection software and services. "Security teams at these retailers need to have playbooks to track and issue takedowns for impersonator profiles, especially if the attackers are phishing or scamming customers," Curcuruto says. "Customer success turns into a security problem if customers fall victim to cyberattacks."

Most importantly, retailers need to train employees to question everything so that attackers can't enter and exploit a retailer's systems because of an employee's misstep.

"Repeat the message in as many ways as possible and keep reminding them with new examples of people exploiting, or attempting to exploit, your systems," he says. "Make sure that what you tell them is relevant and not just

'CYBERCRIME IS LIKE A BALLOON. SQUEEZE ONE END AND IT BULGES WHERE THERE IS THE LEAST RESISTANCE.'

CHRISTIAN JANOFF, SECURITY SOLUTION ARCHITECT AT CISCO

generic situations where they can't see how it relates to them."

Grove recommends retailers regularly review their security policies. "Technology is evolving and you have to move with it or it will be used to exploit you," he says.

Because it can be hard to keep up, many retailers, including Find Me A Gift, consult with security specialists and use vendors' tools. But in order for those to help, retailers have to properly implement them, Grove says. "There is no point in paying for an expensive antivirus software if half your staff then disables it or never installs it."

BUT WHAT, EXACTLY, DOES BETTER cybersecurity preparedness and a better security posture look like in online retail? To start, online retailers need training on online fraud tactics and defenses, and to make greater investments in security technology and third-party risk management services that match their level of risk and tolerance of fraud losses, says Randy Vanderhoof, executive director of the Secure Technology Alliance, a security-focused trade group. For example, an online digital goods vendor selling ringtones may tolerate more fraud than a high-end jewelry merchant because the cost of goods for fraud losses are much higher for the jeweler, he says.

Retailers also need to share information with each other, he says. While the Retail Industry Leaders Association in 2014 worked with retailers including Gap Inc. and Walgreen Co. to launch an intelligence-sharing resource enabling merchants to swap information on breaches and looming threats, many retailers don't disclose the threats they're battling.

Attaining "real cyber resilience is a daily struggle, and thus requires daily investment," O'Sullivan says. To mitigate the occurrence of misconfigurations that could give criminals a way into a retailer's IT systems, enterprises must consider that the biggest risk lies in not knowing exactly how their systems operate, he adds.

Ultimately, most online retailers, especially small and midsized companies with limited resources, cannot implement and maintain an effective fraud prevention system on their own, "so partnering with a managed fraud provider who also takes on responsibility for any fraud losses is the best path forward," Graff says. While these providers may cost thousands of dollars a year at first (and potentially more depending on the size and risk profile of the online retailer), he says that "a single bad month as the result of an attack can have a devastating impact on a business's financials for a year."

"The costs to recuperate after an attack often far exceed the cost of continued preventative measures, not to mention the damage an attack can have on brand loyalty," Graff adds. "Fraud must not be seen as an unavoidable risk, but as a predictable expense." Last year, the average cost of a data breach was $1.3 million for large companies, and $117,000 for small and midsized businesses, according to research by Kaspersky Lab, a cybersecurity and anti-virus developer based in Russia.

With so many of these cyber-exploits relying on basic human manipulation, O'Sullivan points out that educating all employees is critical. Online retailers need to train and regularly test employees on the subject of social engineering, as seen with phishing emails, which often look identical to valid messages from higher-ups.

"This can have a real impact in reducing the ability of malicious actors to extract information from enterprises," O'Sullivan says. "Another specific measure would be that retailers mandate ongoing monitoring of any third-party vendors' IT assets, to ensure that bad guys do not gain access to retailer data through an insecure partner."

KAREN EPPER HOFFMAN IS A FREELANCE WRITER BASED IN OLYMPIA, WASHINGTON.