SALES BOOST

By Sara Lavenduski

Become Savvy With Cybersecurity

Think only the big guys have to worry about digital attacks? Think again.

INSIDE THE SECTION

INDUSTRY SNAPSHOT

The Cybersecurity Challenge

As malware attacks become more prevalent and costly, promotional firms face a critical moment.

BY CHRISTOPHER RUVO

Les Dorfman calls it "probably the worst virus" he's ever seen in his 35 years in the industry.

Last April, Dorfman's company, High Caliber Line (asi/43442), was attacked by malware that repeatedly disrupted the supplier's systems over several days. The virus arrived in emails that appeared to be from customers, asking recipients to click on a link to complete a shipping form.

"It spreads very rapidly throughout your computers and servers," says Dorfman, High Caliber's EVP.

Working around the clock, the IT team at High Caliber removed the malware – a "Trickbot" that can generate and rapidly download other viruses leading to dreaded blue screens. This particular virus was complex: it hid in several places, including the "C Windows" directory and "net defender" folders.

After the virus was accidently triggered again, High Caliber staffers were forced at times to manually fulfill orders. "Everyone needs to be aware that this is out there," says Dorfman.

Major data breaches within global giants like Yahoo, Facebook, Marriott and Equifax have been part of a surge in global data breaches the past three years, and the same phenomenon is hitting this industry. The malware that attacked High Caliber (which ultimately defeated the virus) also attacked distributors and suppliers, although only a handful publicly acknowledged the attacks, including Top 40 suppliers Hub Promotional Group (asi/61966) and Hit Promotional Products (asi/61125).

In January, Discountmugs.com (asi/181120) alerted potentially affected customers about a cyberattack that siphoned off customers' credit cards and other personal information with a malicious code inserted into the company's shopping cart page. The data breach lasted from August 5, 2018 through November 16, 2018. When DiscountMugs.com discovered the code, "We immediately removed the unauthorized code and reported the matter to law enforcement and to the payment card companies," CEO Sai Koppaka said.

In September, supplier Colorado Timberline ceased all operations indefinitely after being "plagued by several IT events" the company said in a notice to customers. "Unfortunately, we were unable to overcome the most recent ransomware attack and as a result, this unfortunate and difficult decision was made."

It's rarely mentioned among the top challenges promo firms are dealing with, but the evidence is mounting that cybersecurity must be addressed. "These data scams are very convincing and can have extremely serious repercussions," Dorfman says. "Major preventive measures have to be taken."

ONLY **33%** OF DISTRIBUTORS WITH $100,001-$1 MILLION AND **41%** OF DISTRIBUTORS WITH $1 MILLION+ TO $5 MILLION IN REVENUE HAVE DATA SECURITY POLICIES IN PLACE, COMPARED TO **74%** OF FIRMS ABOVE $5 MILLION. (ASI)

Timeline of Notable Attacks

While breaches have been increasingly reported in the U.S. in recent years, the promo market faced significant attacks as far back as a decade ago.

September 2008
Hackers raided **Newton Manufacturing's** systems several times, obtaining the social security numbers of certain clients. The attacks were found during an audit at Newton.

August 2009
Gateway CDI suffered a significant summertime breach, leading its client Mozilla Firefox to temporarily shut down its online store, which sold promotional items like T-shirts, mugs and mouse pads.

November 2009
A late-year attack overloaded servers at supplier **Leed's** (asi/66887), disabling the company's main website for several days and disrupting the firm's overall business.

June 2015
Casad Company (asi/168375), which runs the site totallypromotional.com, reported hackers accessed the credit/debit card info of some customers. Casad learned of the breach after customers saw unauthorized charges on their cards.

February 2018
A ransomware attack took **HALO Branded Solutions'** (asi/356000) ERP system offline for two weeks. Company reps had to communicate with clients using their personal email addresses.

April 2018
The same malware attacked systems at supplier **High Caliber Line** (asi/43442) multiple times over four days, forcing the company to keep up with orders manually.

April 2018
A virus disrupted the computer systems at **Hit Promotional Products** (asi/61125), targeting a protocol on one of the supplier's file servers that processes artwork.

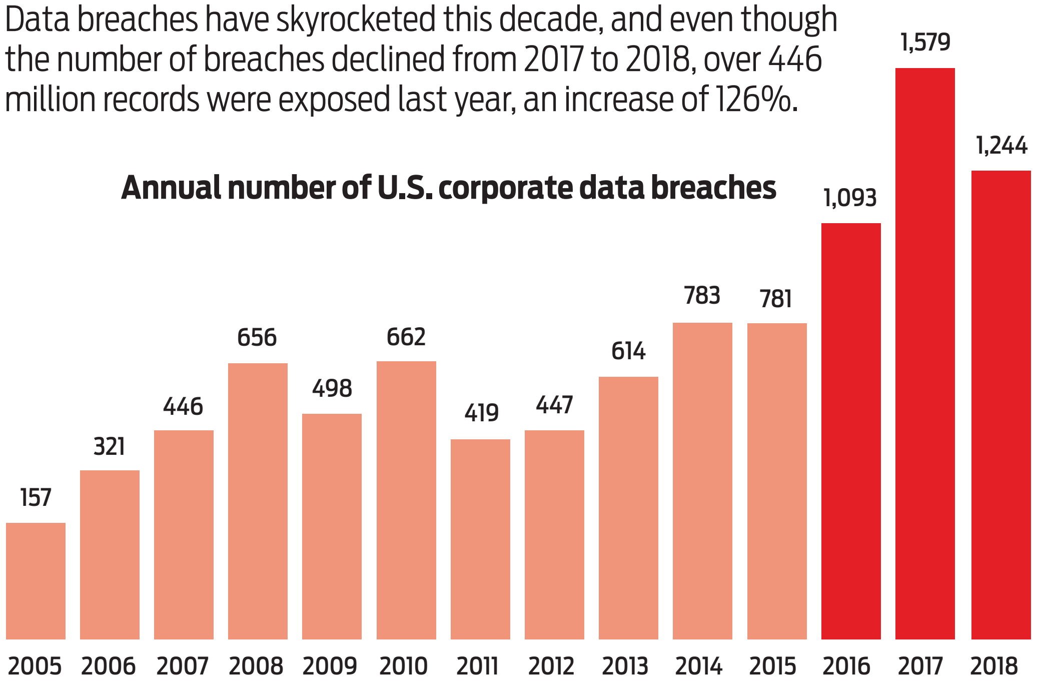
September 2018
Colorado Timberline closes after several IT events and ransomware attacks.

January 2019
Discountmugs.com (asi/181120) reveals a site breach that resulted in the potential exposure of customer credit card numbers and personal information.

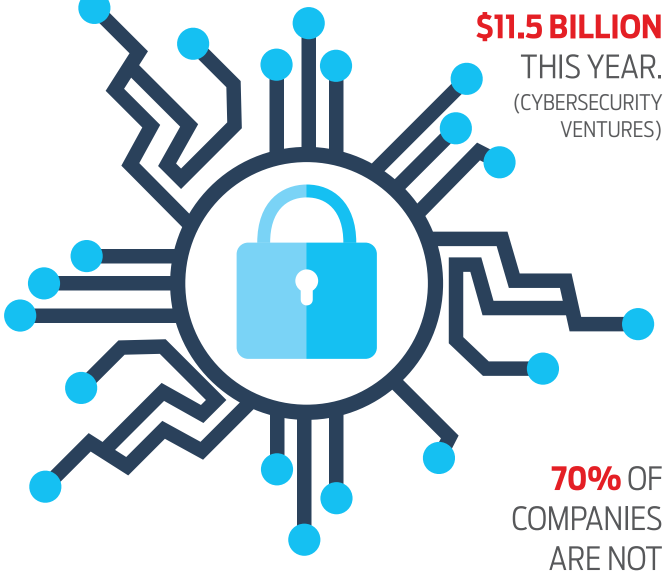
STATISTICS

At Risk

Data breaches have skyrocketed this decade, and even though the number of breaches declined from 2017 to 2018, over 446 million records were exposed last year, an increase of 126%.



Source: Identity Theft Resource Center



GLOBAL COSTS OF RANSOMWARE ATTACKS WILL HIT **$11.5 BILLION** THIS YEAR. (CYBERSECURITY VENTURES)

70% OF COMPANIES ARE NOT PREPARED FOR A CYBERATTACK. (HISCOX)

33% OF EMPLOYEES SAY THEIR EMPLOYER HAS PROVIDED NO CYBERSECURITY TRAINING. (ESET)

Cybersecurity Best Practices With ASI's CTO Dave Lakshmanan and VP of Infrastructure Services Seth Kusiak

Q: What protections should companies have in place?
DL: For smaller companies, save customers' information in a place only you have access to. Password-protect the files containing sensitive information. If any employee leaves a company, terminate their access and change passwords to the systems they had access to.

SK: Install all the latest security updates. Use unique passwords for each website/service you use, perhaps using a password manager like 1Password. Register for free to be notified of data breaches involving your email address with Have I Been Pwned; IT staff can also do this for any email address in their company's domain. For larger companies, ensure that users don't have admin privileges on their computers, and control the software, including browser extensions, installed on computers. All companies should ensure that backups of critical systems are performed and successful recovery of that data is periodically tested.

Q: What should staff know?
SK: Your employees are the first line of defense – they receive malicious content that wasn't blocked by security controls. Security Awareness Training is essential in helping employees identify common phishing and social engineering attacks. I recommend the training created by PagerDuty, which they've open-sourced at sudo.pagerduty.com, so any company can customize its own training program. We can't overstate the importance of the relationship between the Service Desk and employees.

Q: What are the consequences of an attack?
DL: There could be a loss of bank, credit card and payment information, resulting in financial losses that may not be recoverable.

SK: Damage to your reputation and trust is bad enough, but severe disruption to operations can also occur – it may be costly, and in some cases, recovery may not be possible. In 2017, Equifax was breached as a result of not installing a security update that had been available for more than two months prior to the incident. Had the security update been installed, the breach, which exposed sensitive personal information of 143 million people, would have been prevented.

Dave Lakshmanan

Seth Kusiak

Q: How should a company deal with an incident?
DL: Have a checklist prepared ahead of time, and always err on the side of caution if you suspect your systems have been compromised. Alert affected parties immediately so they can cancel accounts or alert banks and credit card companies, and change passwords to all access points.

SK: Consider having cyber insurance and understand what's covered in your policy.

EXPERT TIPS

Safe and Secure

Follow these suggestions to mitigate your chances of being impacted by a cyberattack.

The Pro: Christopher Emerson
Title: CEO
Company: White Oak Security, Plymouth, MN

There are many types of cyber threats out there.

"One of the most common ones is phishing, where you receive emails that say 'Wire me money quickly,' or 'Download this PDF document, it's totally safe, trust us.' With really sophisticated emails, it's difficult to discern whether or not they're legitimate, so it's easy to accidentally click on them. Another type is ransomware, where a hacker encrypts your entire hard drive and demands bitcoin, basically taking it hostage. The third is account takeover (ATO), a type of network breach where a database is made public and hackers go in and take account and website information."

Recognize the warning signs.

"If an email asks for sensitive information and you're not expecting it, that's a red flag. If you get an email from someone you know and the format is unfamiliar, or if there are grammatical mistakes, or there's an unusual sense of urgency, like they ask for your social security number or threaten to disable one of your accounts, that's suspicious. A lot of ransomware originates from phishing emails. It will ask you to download data, usually in the form of an attached document. Also monitor network log-in attempts. If your business hours are 8 a.m. to 5 p.m. and you see attempts at 2:30 a.m., or a large number of failed attempts, like 7,000 at a time, it could be someone trying different combinations of credentials hoping something works."

Have protections in place.

"Endpoint Data Protection secures a network's endpoints, like employees' desktops, laptops and mobile phones. Firewalls block unauthorized access to a network. Review log-in records regularly, and have multifactor authentication measures in place, especially if they're outside-facing. It's also important to have a security awareness program for staff education. Host lunch-and-learns, send out reminder emails, or leverage someone at the company who's passionate about the issue and can provide information."

Build a culture of trust.

"If an employee accidentally clicks on a phishing email, you want them to tell you. They shouldn't be afraid you'll be angry with them. Say 'Thank you, this allows us to respond more quickly and lessen the impact.' The sooner the IT team is made aware, the shorter the time to detection. Looking down on employees exacerbates future issues."

The consequences are serious.

"Some companies have gone out of business. Cisco reports more than half of companies hit by cyberattacks spend over $500,000 dealing with it. For 20% of companies, it costs $1 million to $2.5 million. By and large, smaller companies aren't as likely to be targeted, but it takes just one. Ask yourself, 'Can we survive a breach? How long could we go before losing business?'"

Know what to do in the event of an attack.

"Get a firm in that specializes in incident response and forensics. Don't turn the computers off; that can destroy the log files that will help you understand the breach. Comply with all federal, state and local obligations, and be upfront with employees and clients. Give them a timeline of when you identified the attack, what this means for them and what you're doing to avoid it again. Don't say, 'We fixed it, nothing to see here.'"

Christopher Emerson is a cybersecurity expert with experience implementing security programs for large companies. He has worked in security and applications at Target, Best Buy and Symantec.

TAKEAWAYS

1

Know the warning signs.

2

Build a culture of education and transparency at your company.

3

Immediately alert appropriate parties if you're attacked.

THERE WILL BE A RANSOMWARE ATTACK ON BUSINESSES **EVERY 14 SECONDS** BY THE END OF 2019. (CYBERSECURITY VENTURES)

WATCH THIS!

In this short TEDx talk, expert Nick Espinosa shares the five laws of cybersecurity, from exploited vulnerabilities to the tendency for people to trust even when they shouldn't, and more. Watch it at bit.ly/5LawsCybersecurityVidASI

DISTRIBUTOR TIPS

No Small Concern

Any company – especially a small business – is at risk from the impact of cyber threats.

The Pro: Randy Mohrbacher
Title: CIO
Company: AIA Corporation (asi/109480)

In its 2018 Data Breach Investigations Report, Verizon found that 58% of cyberattacks target small businesses. While the reward might not be as high, hackers have a better infiltration success rate because small and mid-size businesses (SMBs) are more vulnerable, with smaller teams and fewer cyber protections in place.

Unfortunately, too many companies mistakenly believe they're too small to be a focus of cyber criminals. "Smaller companies think, 'What could we possibly have that hackers want?'" says AIA's CIO Randy Mohrbacher. "But that makes them an easy target." It's all the more reason to implement cybersecurity protections to help safeguard firm and client data.

Many of the successful infiltrations originate with opening phishing emails and clicking on a link or downloading a malicious file that looks legitimate. And with hackers becoming ever more sophisticated, bad emails are becoming increasingly harder to flag.

"It's easier to infiltrate a company through email because business runs off of email," says Mohrbacher. "The recent problems at some of the big industry suppliers originated with someone clicking on a link and the threat went undetected. It gets in on one computer and spreads to others. I recommend training and increased awareness, having an active protocol and regularly scanning computers, networks and data."

Mohrbacher also recommends enlisting a security specialist to do regular monitoring and address issues as they arise. "I tell companies not to go this alone," he says. "Even if you think you took care of one threat, you still might not be sure what else it may have affected."

Of course, cost for protection can be a question, particularly for SMBs. But Mohrbacher says to think about the cost of not having protections in place instead. "A reasonable cost is relative when you're looking at potential losses," he says. While costs vary widely depending on type and need, Mohrbacher says anti-malware is about $20-$30 per computer, as one example, while company training on recognizing threats can be about $1,200 a year. Meanwhile, recovering from an attack can cost $100,000 and above, and according to the National Cyber Security Alliance, 60% of SMBs go out of business within six months after being hacked.

"It's better to be prepared and avoid the mess in the first place," he says. "There are thousands of these threats, and they might look similar to the last one or it's a new variant. Make sure you're regularly updating your anti-malware and operating system."

The team at AIA actively monitors all tech assets and networks. Mohrbacher says they stop cyber threats several times a month, a lot of them coming from China. "People are focused on their business, so this isn't as much of a focus sometimes," he says. "But if a threat hits, it all goes out the door."

If an attack does impact a company, there are specific steps for handling the situation.

"First is to remain calm," Mohrbacher says. "People lose it because they're in a panic, and it's understandable because this is their livelihood. But stay calm and make an inventory of the data on your networks and computers. Contact local and national experts to assess the damage and work on recovery. And regularly back up your data as a part of company protocol so you can restore as much as possible. You might lose a couple days' worth of transactions, but it's better than everything."

Matt Gresge, president & CEO of AIA, says that the new reality of cyber threats is forcing companies to be aware and proactive. "This is now at the top of our agenda," he says. "It's up there with capital structure and HR policies. It's no longer an esoteric afterthought."

CYBERSECURITY ATTACKS TYPICALLY COST SMALL BUSINESSES BETWEEN **$84,000 AND $148,000** EACH. (UPS CAPITAL)

TAKEAWAYS

1

SMBs are often easy targets for hackers.

2

Internal teams need to be on the lookout.

3

Just one attack can put a company out of business.

LISTEN TO THIS!

small business CYBERSECURITY PODCAST

In this episode of the Small Business Cybersecurity Podcast, hosts Stephen Zetzer and Femi Dada discuss the importance of training employees as one of a company's first defenses against cyberattacks. Listen to it here: bit.ly/SmallBizCybersecurityPodcastASI

SALES BOOST

INDUSTRY STRATEGIES

Safety Measures

Promo IT leaders and executives weigh in with essential tips for keeping your company safe.

BY CHRISTOPHER RUVO

Cyber threats are an inescapable reality in the age of digital business. Last spring, the onslaught of malware attacks on promo firms occurred amid warnings from government cyber security officials in the U.S. and U.K. that Russia-backed hackers have their sights set on western businesses and individuals. Whether or not the Kremlin has been behind the attacks on promo firms is unknown.

Here, executives and IT experts in the promo industry share a few best practices businesses can use as bulwarks against cyber incursions.

Use a Secure Email Gateway Like Mimecast: "Email is often the Trojan Horse of malware getting into your network," says Marc Sule, CIO at Top 40 supplier alphabroder (as/34063). "A secure gateway can lower your risk by monitoring and blocking users from opening malware attachments or clicking bad URLs."

Utilize Malware-Scanning Software: This software manages anti-malware policies, routinely scans corporate systems and PCs, and alerts your IT team when malware is detected. "These services can be configured to automatically quarantine or eradicate the malware before it can spread," says Sule. He's partial to Microsoft's SCCM Endpoint Protection. "Endpoint Protection helps prevent targeted attacks," says Greg Muzzillo, founder of Top 40 distributor Proforma (asi/300094).

Build Sturdy Walls: Firewalls are network security systems that monitor ingoing and outgoing network traffic, creating a barrier between the secure internal network and the untrusted external network, like the internet. "It's critical to have a properly configured next-generation firewall with unified threat management," says Muzzillo.

Install Anti-Virus Protection on All Computers: The protection should be updated in real time, and all systems must be up-to-date on patches and feature strong spam filters.

Have Good Back-Ups in Place: If a breach occurs, this is essential to recovering as much data as possible. "Always back up your critical systems on a separate virtual local area network (VLAN) away from the production system," says Sule. "If your production systems and logical backups (or even disaster recovery environment) all exist on the same VLAN, ransomware may be able to encrypt them all. Backups add redundancy and allow for business continuity and recovery."

Quarantine Infected Devices and Systems: "Isolate the infected machines," says Sule. "Sever the network with a satellite office that has been infected to protect other locations. This certainly could result in impacted operations, but that's better than an attack spreading across your network." An infected device should be wiped and restored, with the restore point being somewhere before the infection.

Utilize the Principle of Least Privilege: Give users access only to files they absolutely need.

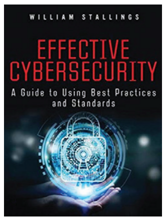
Be Password-Savvy: Employees should engage in safe password practices to make them harder to guess ("123456" and "password" don't cut it) and use different ones for all accounts. In addition, two-factor authentication adds an extra layer of security.

Analyze Email Addresses: Tell employees to pay attention to the "To" and "From" fields in their received emails, says Muzzillo. Is the "From" email address long and/or not apparently linked to a recognizable address? Does it have spelling errors or in other ways seem suspicious? "These are warning signs of a phishing scam," Muzzillo says.

Implement a Training Program: The growing sophistication of scams means even seasoned corporate employees and CSRs can be persuaded to give out passwords, account numbers or other sensitive data that can be used to access systems and/or perpetuate identity theft. Alphabroder, for example, contracted with a company that provides anti-phishing training and mock phishing campaigns to monitor, score and identify additional training needs within its corporate user base. Also, make it part of official company policy that sensitive or confidential information should never be sent via email or unfamiliar websites.

WHILE 91% OF PEOPLE KNOW THAT PASSWORD RECYCLING IS A SECURITY RISK, 59% USE THE SAME PASSWORD FOR ALL THEIR ACCOUNTS. (LOGMEIN)

READ THIS!



This new instructional book gives readers the low-down on the required technology, operational procedures, management practices and protocols for successful cybersecurity. Author William Stallings includes detailed tutorials, learning objectives, keyword lists and information for further resources. Find it at bit.ly/EffectiveCybersecurityBookASI