Is Your Small Business the Victim of a Cybersecurity Breach?

Comerica Bank®

Comerica.com

Contents

Introduction 01

Always be on the lookout for signs 02

Mobilize a response team 03

Patch vulnerabilities and reinforce defenses 04

Prepare public response and notify customers 05

Make sure it doesn't happen again 06

Introduction

The proliferation of cyberthreats has created a problem for small businesses. Even when they construct defenses to protect their operations, their data and their customers, small businesses very often find themselves the victims of attempted breaches, if not outright attacks and infiltration.

According to a 2018 report from insurer Hiscox, 47 percent of small businesses experienced a cyberattack within the past year. Of that group, 44 percent suffered between two to four attacks. Those statistics paint a sobering portrait of the situation at hand. If you're a small business, you have about the same chance of being attacked as correctly calling heads on a coin flip — which is to say nothing of the rather high odds for being hit by multiple intrusions.

Reality is if you're a small business, there's a big likelihood that you'll be hit with a cyberattack at some point. So the question is: How prepared are you to deal with it? If somehow your defenses are compromised and an incident occurs, you must have a plan of action ready. This need is essential to basic business continuity in the modern age. Here's what small businesses should know about responding to a cyberattack.

Always be on the lookout for signs

Some attacks — like ransomware — may be obvious in nature. Other attacks are conducted on a stealthier basis and might not show outward signs. Even worse, a small business could be hit by an inside job and not catch any wind of the subterfuge until it's already too late.

It's crucial for small businesses to be observant in order to be responsive. Verizon's 2018 Data Breach Incident Report found 87 percent of compromises occur within minutes, but just 3 percent are caught as quickly. Much more worrying, 68 percent went uncaught two to three months after the event. Look for signs like unusually slow networks, abnormal activity or changes in files.

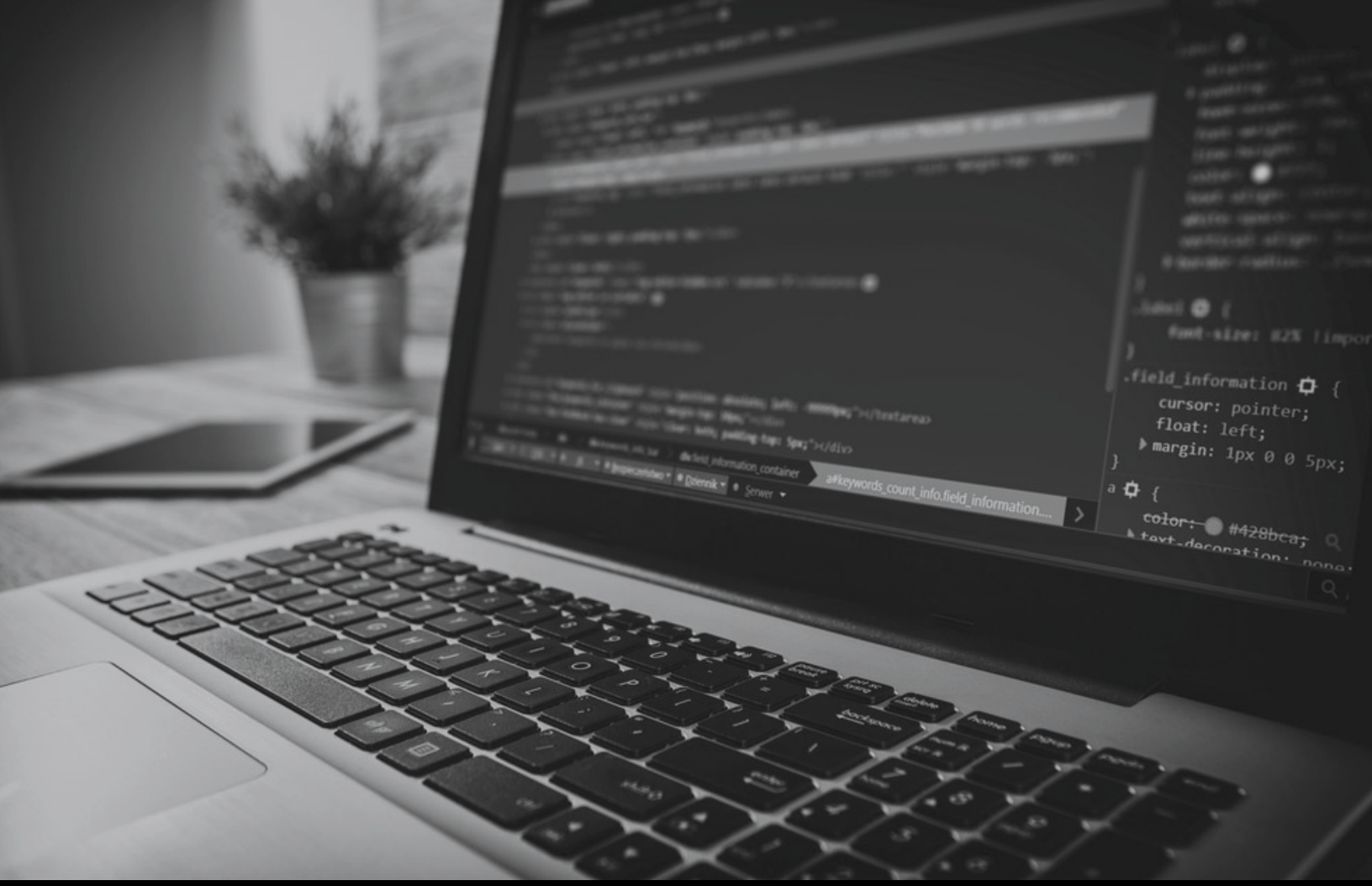
Mobilize a response team

Once a small business has the slightest inclination that an attack has occurred, it's paramount they mobilize a team as quickly as possible to address the threat and secure networks, data and accounts. The first priority of this team is to contain the breach and prevent any further loss. If you have the in-house IT resources — which not every small business does — then direct the full force of your manpower at securing the business. If necessary, reach out to an IT firm that can help.

The next step is to launch a cybercrime investigation. Basic questions you'll need to answer include:

- When did the event occur?
- How long has it persisted?
- What was accessed, affected or stolen?
- Can any origin or malevolent actors be identified?

The Federal Trade Commission says it might be of benefit at this point to consult a specialist in data forensics, as well as consult with legal counsel.



Patch vulnerabilities and reinforce defenses

Depending on the severity of the attack, it may be best to conduct repair work alongside a cybercrime investigation if possible: You don't want to waste any time in fixing your weaknesses and installing new protections. Contact any involved parties, like solutions vendors or internet service providers, to see what help they can offer. Unpatched vulnerabilities are often a big entryway for hackers, so make sure every system is up-to-date in terms of security. If you need to beef up your cyber perimeter, consider shopping around for advanced products or services.

If you didn't have back-ups installed before the incident, it's a good idea to procure some during this recovery stretch. Such installations are critical to continuity should a business be negatively impacted by an intrusion or theft.

Prepare public response and notify customers

Dealing with a cyberattack internally is no walk in the park, but no business looks forward to communicating that event to customers and the outside public. This can be the most challenging stage of response for small businesses. No matter how the attack transpired, the public doesn't forgive easily, and companies can endure reputation and social media backlash that can have a serious and negative effect on the bottom line.

Still, there is no alternative but to notify customers, business partners and other stakeholders of what happened. A crisis communication plan begins with a company statement about the facts, the steps taken to rectify it and any further action. It's best practice to disseminate the message across different channels, including press releases, social media and media appearances, if applicable. Small businesses have to get out in front of the incident, and that all lies in formulating an effective and honest crisis response.

Additionally, be aware of laws governing how quickly public notifications must be made. For instance, small businesses with customers in the European Union are bound by the General Data Protection Regulation (GDPR) to process a notification within 72 hours of becoming aware of a breach.

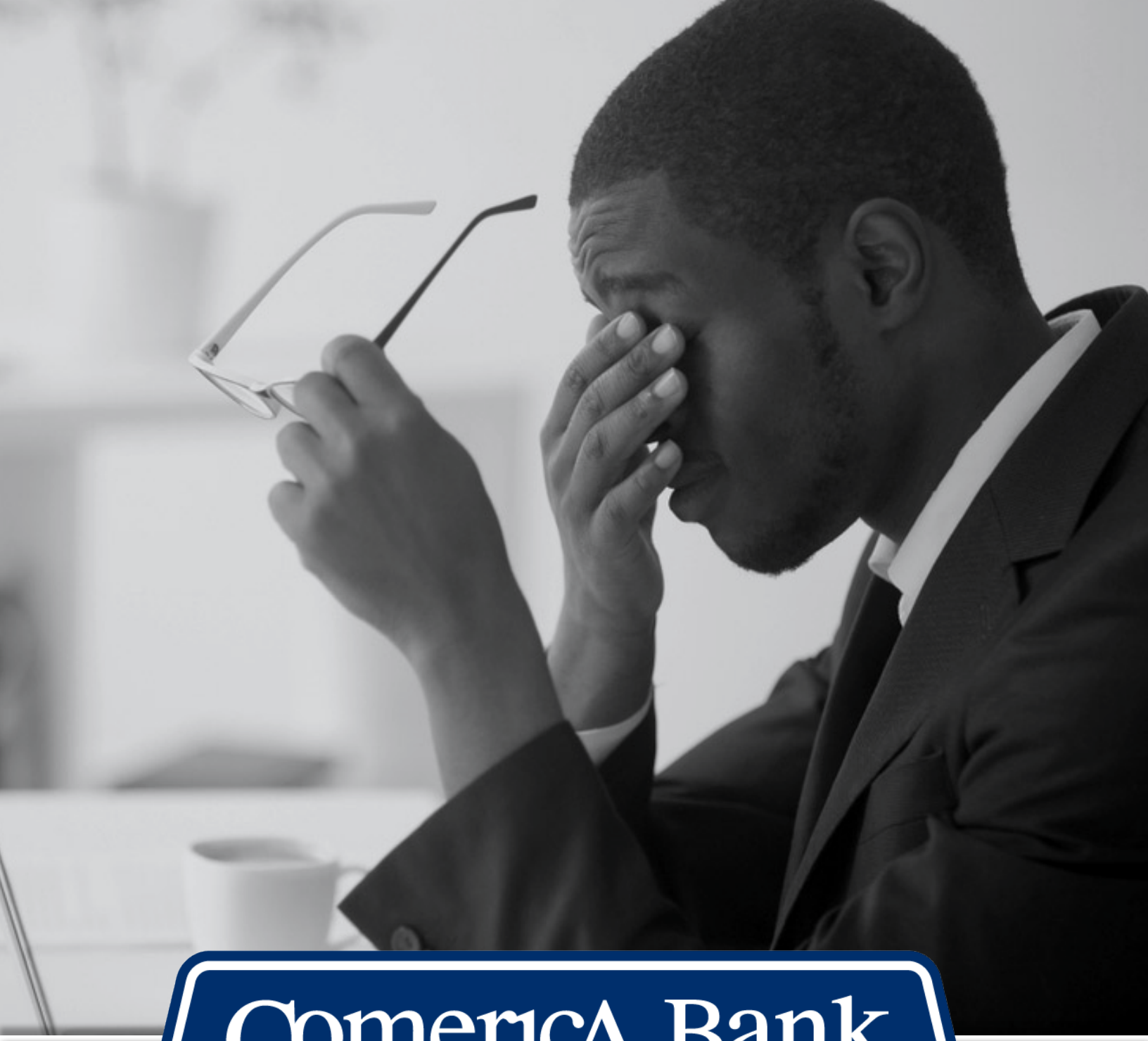
Make sure it doesn't happen again

Small businesses hit by a cyberattack desperately want to avoid another one, yet the Hiscox data makes it clear not everyone will be so lucky. That being the case, small businesses have to be vigilant in protecting themselves and their customers from another attack.

One of the biggest issues to focus on is personal devices used for work purposes. It's largely impossible to avoid the use of a personal smartphone to look up work email (especially with the growing popularity of remote workforces), but employees unwittingly clicking on a phishing link can expose the entire business. That means companies will have to craft rigorous bring-your-own-device (BYOD) policies to protect sensitive data and information.

Altogether, there are a number steps businesses must take in the wake of a cyberattack, each as crucial as the last. Having an informed, resolute response to an attack is a requirement for any small business to protect operations, customers and reputation.

Speak with a Comerica Bank professional to learn how the proper funding may help equip your business with proper cybersecurity protection.



Comerica Bank®

Sources:
https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf
https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf
https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf
https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf