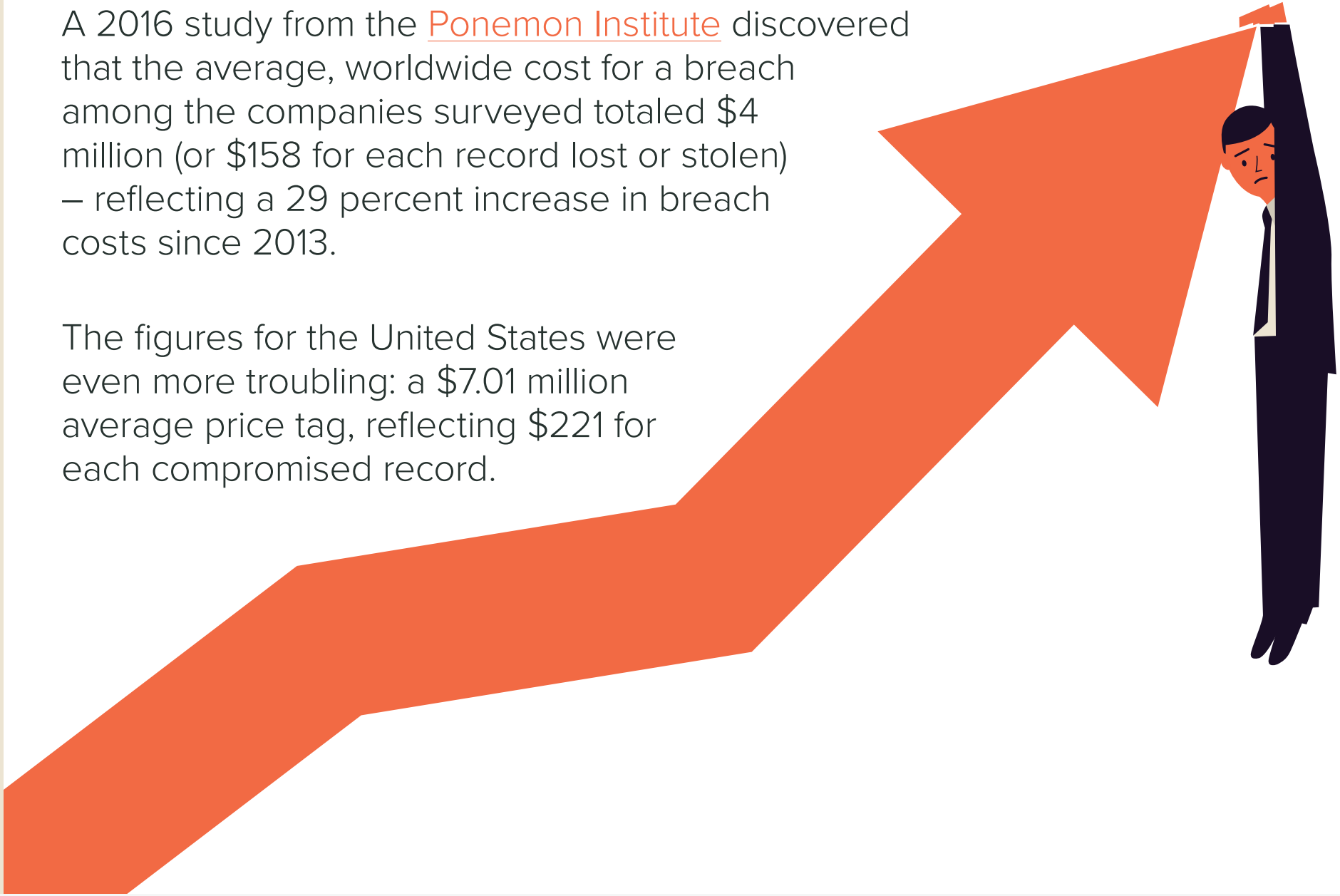
DATA BREACH DISASTERS

How to Prepare for the Worst and Respond at Your Best

The High Costs of a Breach

A 2016 study from the Ponemon Institute discovered that the average, worldwide cost for a breach among the companies surveyed totaled $4 million (or $158 for each record lost or stolen) – reflecting a 29 percent increase in breach costs since 2013.

The figures for the United States were even more troubling: a $7.01 million average price tag, reflecting $221 for each compromised record.



A Matter of Time

While you may be confident that your network and data are currently secure, the findings of the Verizon 2016 Data Breach Investigation Report might give you pause.

In 93 percent of recorded breaches, the attackers only needed minutes to compromise systems. On the other hand, 83 percent of organizations that documented breaches needed weeks to discover the intrusion – and most frequently customers or law enforcement were the source of the alarm.

The Ponemon report also recognized a steady increase in the frequency of cyberattacks, estimating that the average business faces a 26 percent probability that it will experience a data breach affecting at least 10,000 records in the next two years.

Given that a cyberattack is almost inevitable, IT security must become a top priority at every organization.

The **AVERAGE BUSINESS** *faces a* **26%** **PROBABILITY** *of a* **DATA BREACH** **AFFECTING** *at least* **10,000 RECORDS.**

Avenues of Attack

The Ponemon study determined that 48 percent of cybersecurity incidents resulted from a malicious or criminal attack. Verizon offers further insight into the more malicious efforts, with most attacks following common strategies that can include:

Hacking

Physical theft of electronic devices containing confidential data or passwords

Social engineering (e.g., phishing emails)

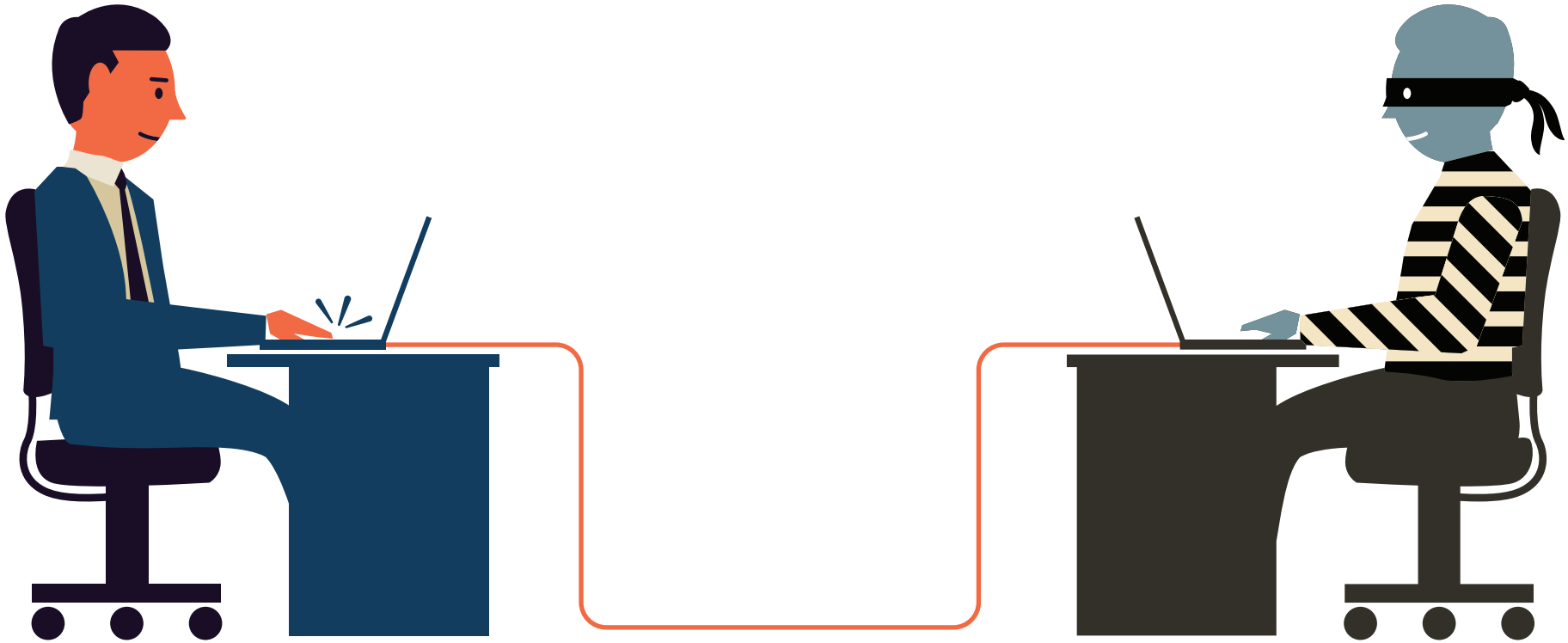
* * * _

Credential misuse (routinely performed by employees inappropriately accessing company systems)

Malware

Another 27 percent of incidents could be tracked to “system glitches,” including IT and business process failures. The remaining 25 percent of incidents were due to employee negligence, such as employees inadvertently sending confidential information to unauthorized parties.

While no cybersecurity program offers a 100 percent guarantee, there are a number of factors that can place your business at increased risk.



Factors for Increased Risk

Naive Employees

Proofpoint research suggests that cybercriminals rely on social engineering techniques as their primary exploit for bypassing network security.

In the past, it was easy to identify phishing schemes because of their poor spelling and grammar, but scammers have grown more savvy. Now, they create targeted spear fishing attacks that address employees by name and use personal details to create an air of credibility.

Phishing
THEN AND NOW

THEN

Dear two whom it shall concern!
Your my lost long friend and I am in need of asistence of the fiscal variety!

NOW

Hi John,
Tom asked me to see if you could forward all of our employees' pay stubs to me.
Thanks!
Bill

Even Mark Zuckerberg, founder of Facebook, fell victim to this weakness. Hackers gained control of his personal social media accounts through his rather simple password of “dadada.”

Weak Passport Policies

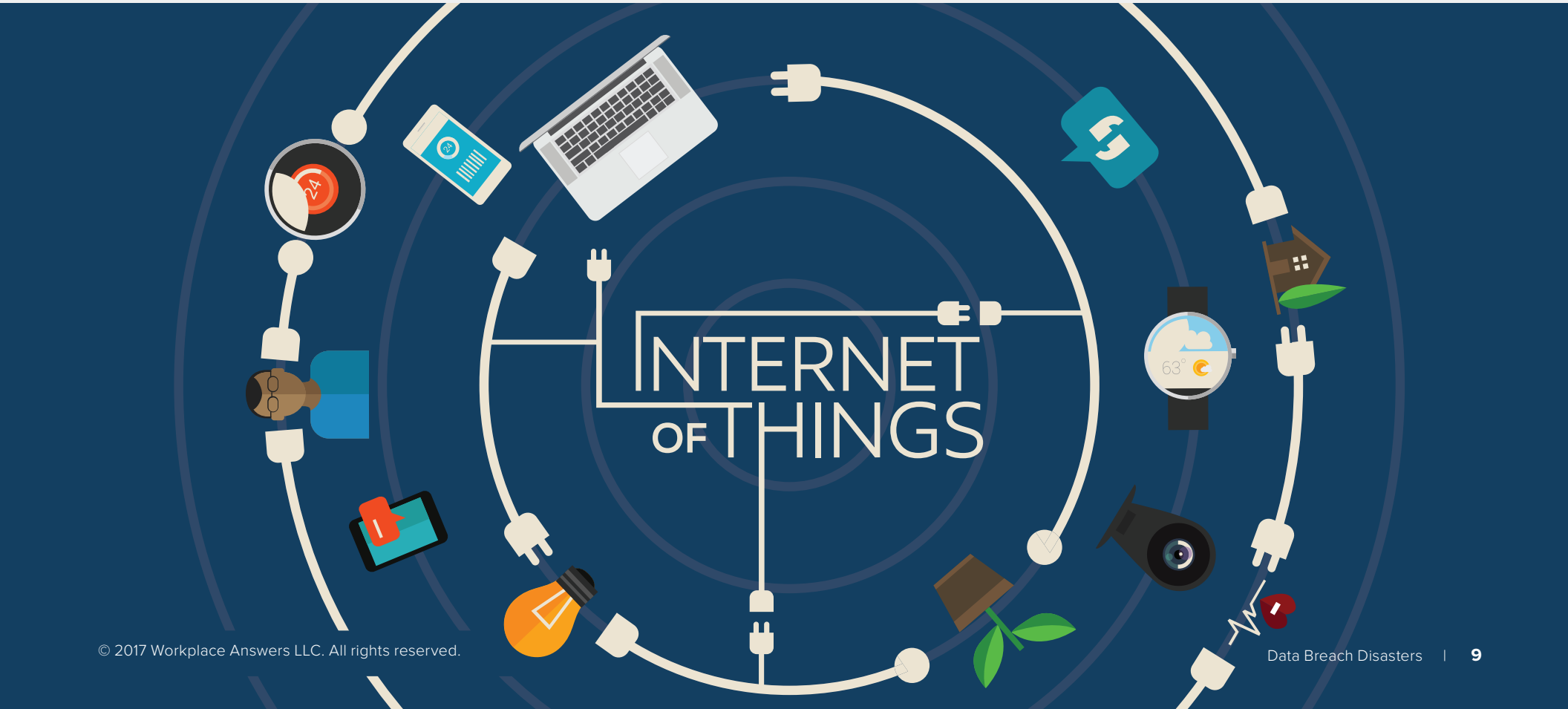
According to the Verizon report, 63 percent of data breaches involved using weak, default or stolen passwords. This fact shouldn’t be surprising, considering a report from SplashData identified the most commonly stolen password in 2015 was “123456,” with “password” being the second most common.

When left to their own devices, your employees will rarely place much thought into your company’s cybersecurity efforts, particularly in password selection.

Internet of Things (IoT) Devices

While the proliferation of “smart” devices may make our lives easier, they pose an increased risk to cybersecurity. Cisco estimates that by 2020, the number of devices contained within the Internet of Things (IoT) will increase to 50 billion.

Many of these devices lack sufficient security measures, which provides cybercriminals with additional tools to exploit during distributed denial of service (DDoS) attacks. In fact, analysts at Gartner, Inc. predict that by 2020, more than 25 percent of cyberattacks will involve IoT devices.



Bring Your Own Device (BYOD) Programs

Similarly, by releasing some of the control associated with how and when your employees access systems and data with a bring your own device (BYOD) program, your company offers new opportunities for criminals and malicious outside parties to attack.

A Crowd Research Partners study found that 39 percent of surveyed businesses had identified malware downloaded to either a BYOD or corporate-owned mobile device, and 24 percent confirmed that employees had connected to malicious Wi-Fi hotspots with these devices.

Also, according to a 2014 survey conducted by Enterprise Management Associates, Inc., 30 percent of respondents who stored confidential company information on their personal mobile devices "frequently" left those same devices in vehicles unattended.

Ransomware

While the explosion of ransomware seems to be slowing, software security firm Trend Micro still predicts 25 percent growth in these attacks.

And no organization should consider itself immune. For example, a Los Angeles hospital had to pay out $17,000 to regain control of its computer systems.

Trend Micro also suggests that ransomware may become a more common component of data breaches. After the cybercriminal has stolen whatever confidential data they can, they'll introduce ransomware to hold servers hostage, further increasing their profits.

What Should You Do Before a Data Breach

Identify Key Targets

More than likely, your business doesn't have an unlimited cybersecurity budget, so it would make sense to place the most protection around your mission-critical systems and data. Perform an internal audit to identify your key systems and their corresponding vulnerabilities, placing particular focus on where a criminal or hacker would focus their efforts.

Records related to consumer interactions are a common objective, given that they regularly include financial data. Tax records, such as employee W-2 forms, also offer an attractive target. These files contain a wealth of personal details regarding employees that hackers can easily mine for fraud efforts and resell to identity thieves.

As part of this evaluation, consult with outside legal counsel and other experts to determine if there are any government or industry-based security mandates for the particular types of data used by your organization. Common examples include:

- Patient data, which is subject to Health Insurance Portability and Accountability Act (HIPAA) requirements
- Credit information, which is managed by Payment Card Industry (PCI) data security standards
- Student records, which are subject to Family Educational Rights and Privacy Act (FERPA) along with 73 state regulations

By better anticipating where hackers and criminals will strike, you can create a more effective security architecture that properly isolates important systems and matches security levels to potential threat.

Make a Response Plan

During a breach, your IT staff are probably going to be too busy to draft comprehensive response plans, so you should draft these ahead of time. With your key targets identified, determine routes of likely attack and develop guidelines for each of those possibilities.

Ideally, any plan should identify how to:

- Contact key cybersecurity personnel quickly
- Determine the order of importance for protecting information
- Preserve records for later investigation
- Determine who should be notified of a breach, including customers or law enforcement

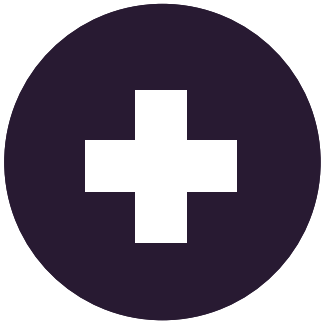
Prepare Your Employees

No matter how well-equipped your network systems are to thwart an intrusion, oblivious employee action can still leave your business vulnerable. To protect your organization, you must thoroughly educate your staff about potential threats and how to avoid them.

After surveying more than 500 executives and security professionals, PwC found that 42 percent of respondents linked security awareness training for new employees with the prevention of potential criminal activities – ranking training as one of the most successful tools for deterrence.

Depending on the nature of your business, there is a strong possibility that you are already legally obligated to provide security training to your employees. The frequency and scope of these requirements vary, but mandated organizations include:

U.S. Federal Agencies



Health Care Organizations

Publicly Traded Businesses

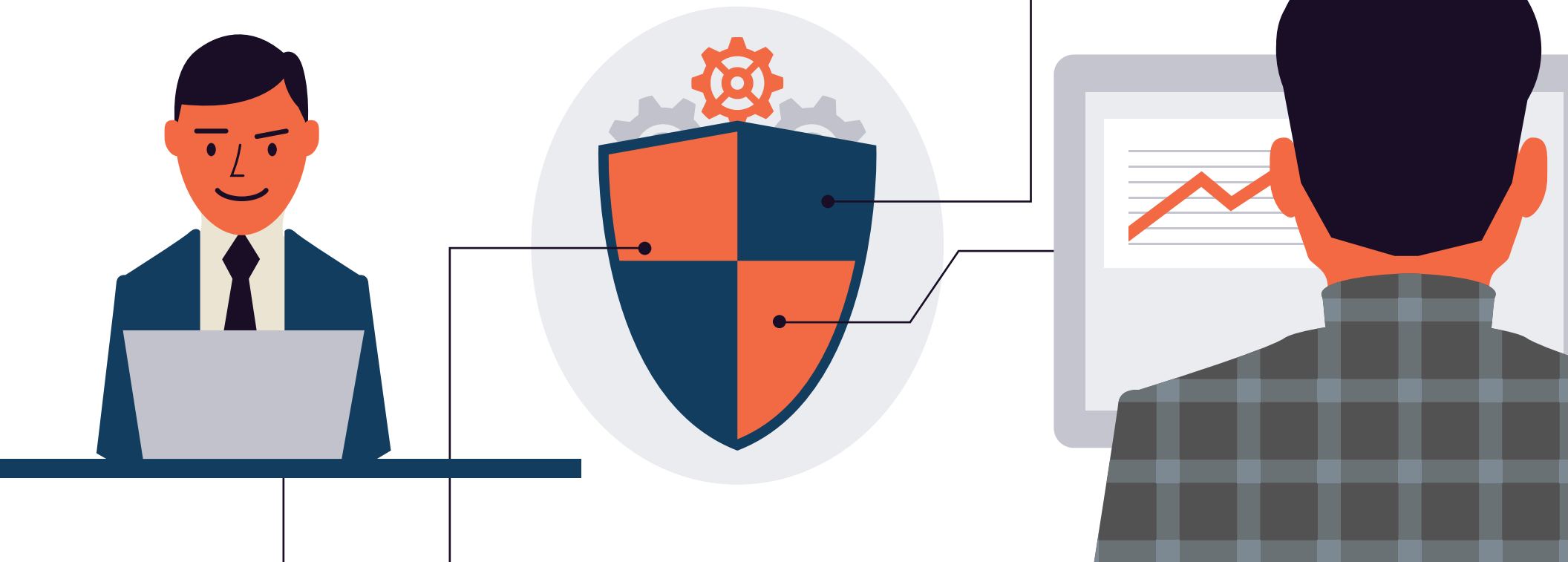
Financial Institutions

Put simply, the modern business cannot afford to omit security awareness training from its cybersecurity budget.

Vet Your Security

Work with your internal IT support staff or outside consultants to regularly assess your existing cybersecurity and scan for vulnerabilities. Conduct frequent penetration tests that include social engineering techniques to gauge how well your systems and employees are prepared to handle common attacks.

The success of these test will not only identify holes in your security policies but can also help to determine which cross-sections of your business may need further education or support.

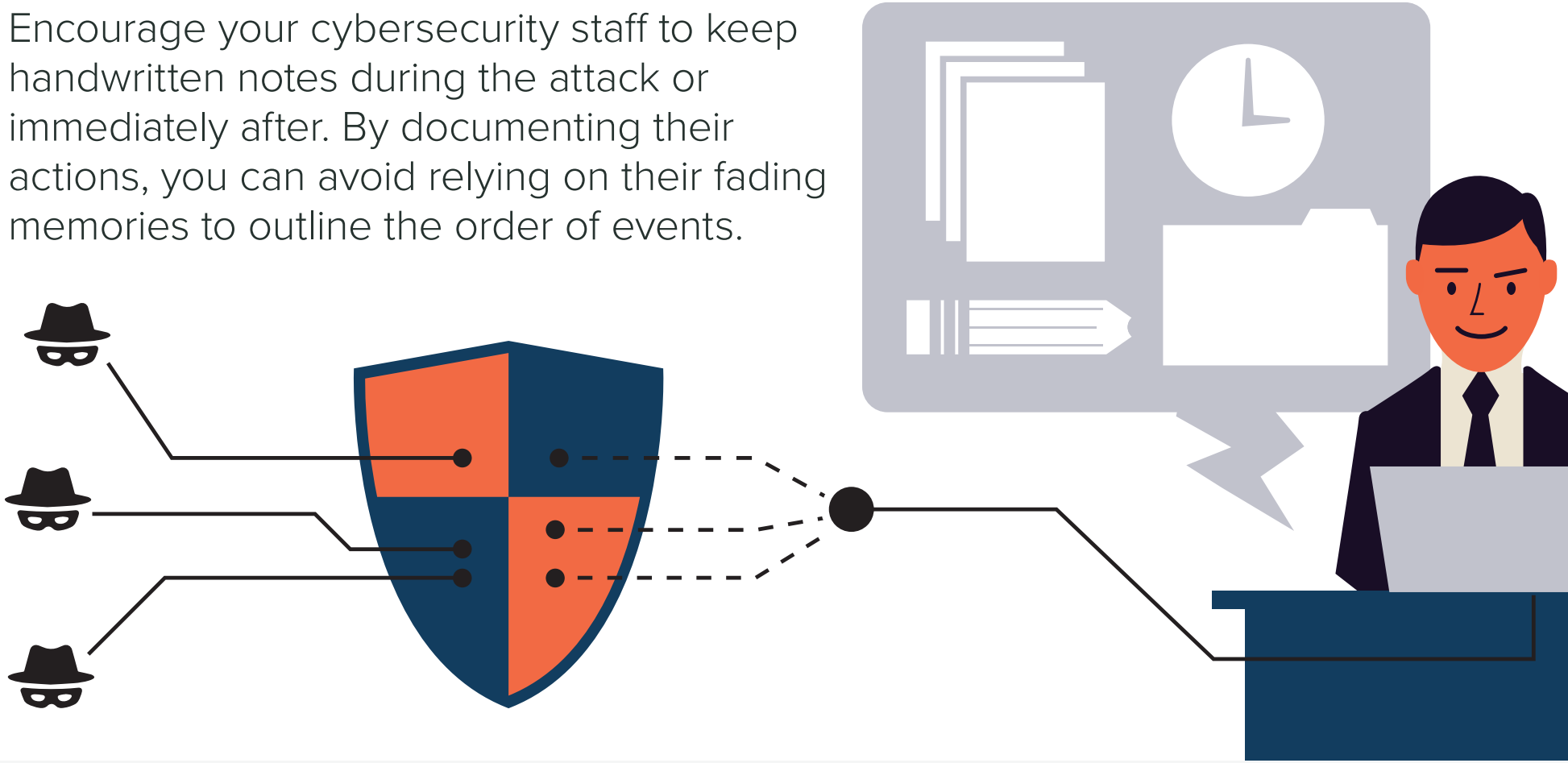


What Should You Do After a Data Breach

Collect Pertinent Information

You should take images of the affected systems and store any related logs or records associated with the breach. Make sure that these items are recorded and stored in a read-only format to preserve the chain of custody should a lawsuit or criminal investigation be pursued.

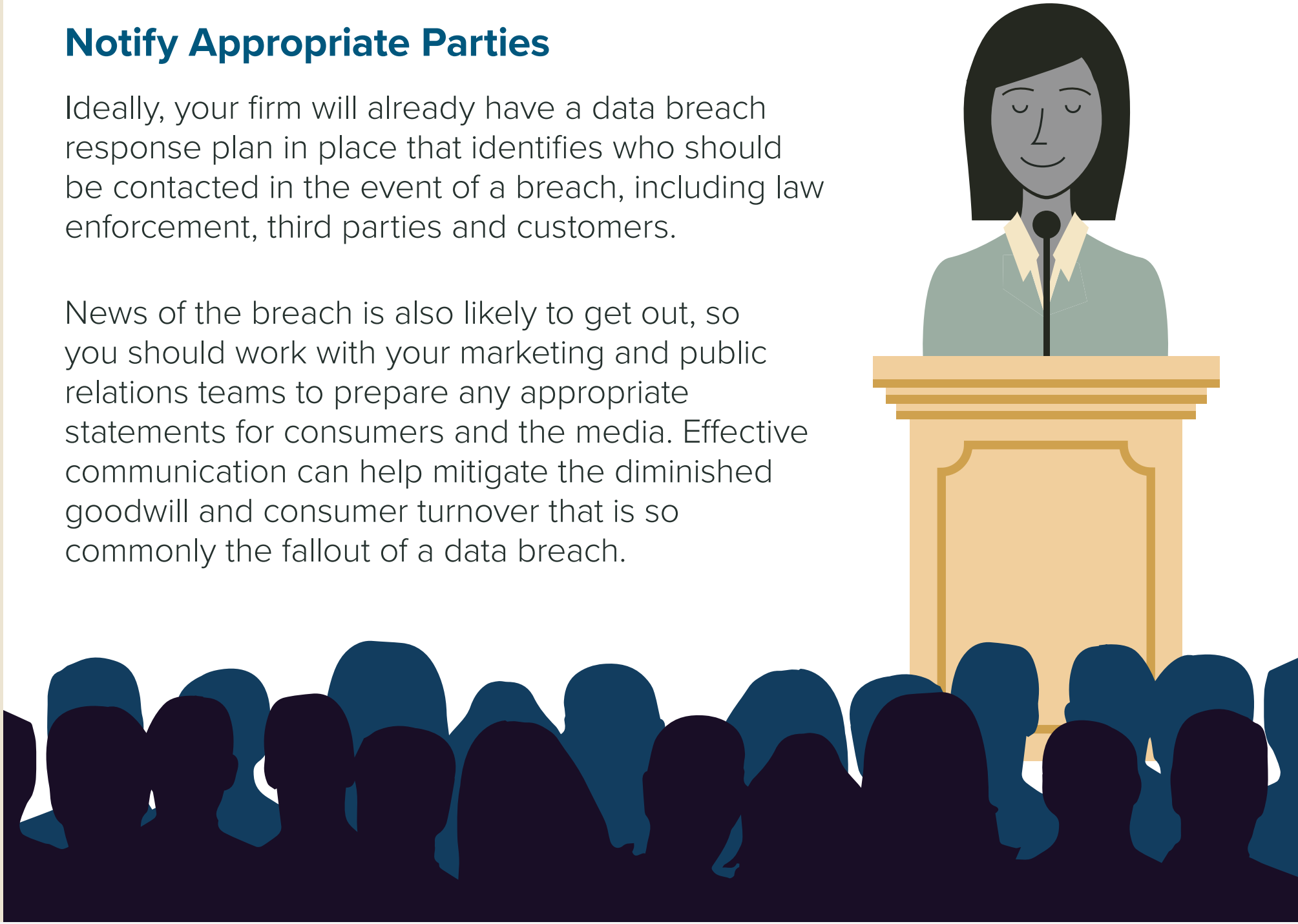
Encourage your cybersecurity staff to keep handwritten notes during the attack or immediately after. By documenting their actions, you can avoid relying on their fading memories to outline the order of events.



Notify Appropriate Parties

Ideally, your firm will already have a data breach response plan in place that identifies who should be contacted in the event of a breach, including law enforcement, third parties and customers.

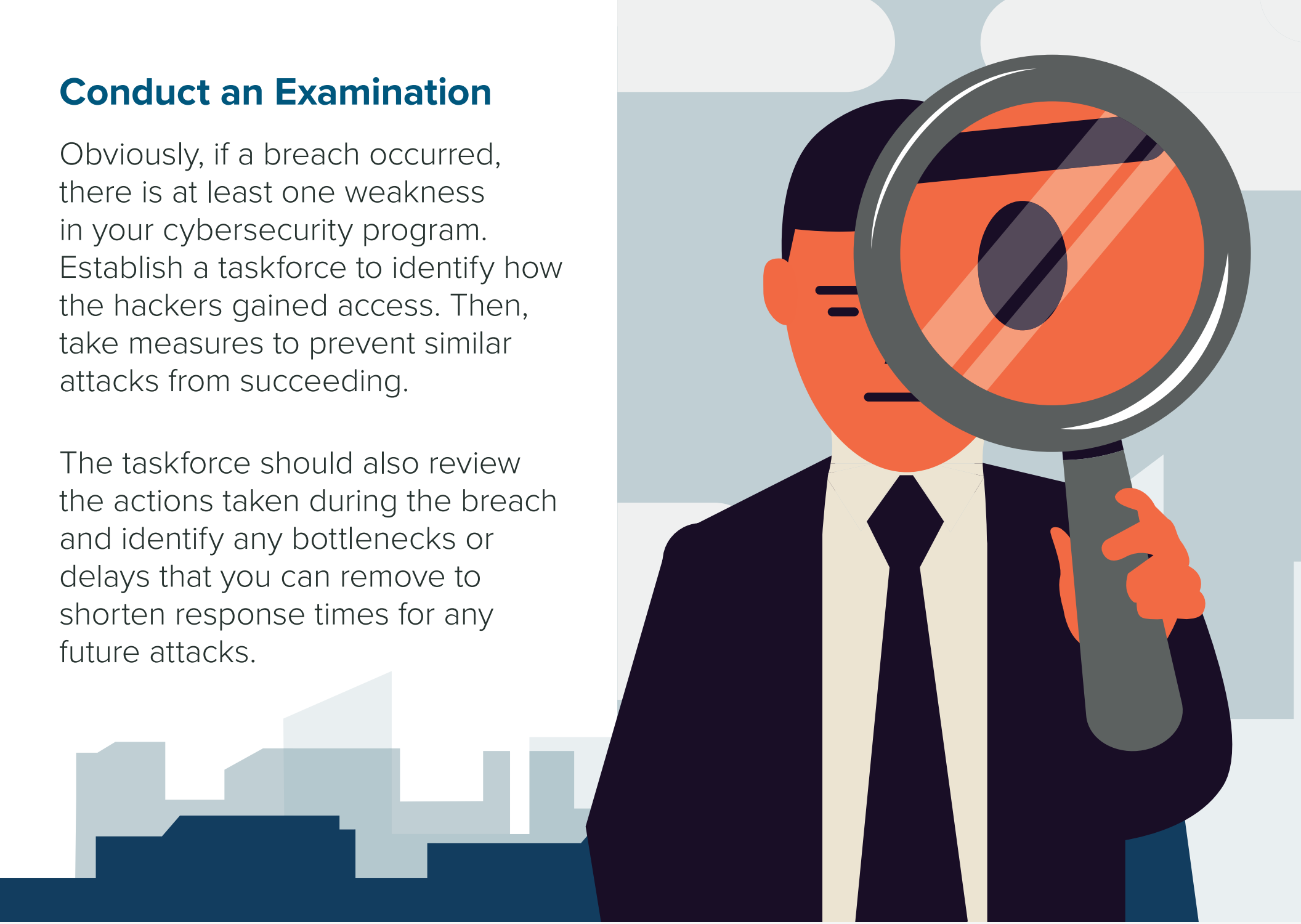
News of the breach is also likely to get out, so you should work with your marketing and public relations teams to prepare any appropriate statements for consumers and the media. Effective communication can help mitigate the diminished goodwill and consumer turnover that is so commonly the fallout of a data breach.



Conduct an Examination

Obviously, if a breach occurred, there is at least one weakness in your cybersecurity program. Establish a taskforce to identify how the hackers gained access. Then, take measures to prevent similar attacks from succeeding.

The taskforce should also review the actions taken during the breach and identify any bottlenecks or delays that you can remove to shorten response times for any future attacks.



Adjust Policies & Budget

Now would also be a good time to conduct a new threat analysis to identify any other potential vulnerabilities that cybercriminals can exploit. If possible, bring in outside experts that specialize in incident response and security gap analysis.

Your organization should also revisit its cybersecurity budget to verify that you are sufficiently investing in preventative measures. The real life example that your business just experienced can better drive home the need for security systems and education to key decision makers.

Revisit Training

Given the statistics, there is a strong chance that the breach was the result of employee negligence, but even if it wasn't, additional training would be a sound idea. Employees vulnerability creates plenty of opportunity for scammers and cybercriminals, and your company's reputation cannot risk another hit – particularly if this next breach comes from a low-level staff member clicking on the wrong link.

Conclusion

There are multiple avenues that criminals and hackers exploit to gain illicit access to your critical business systems, and no protection is foolproof. Furthermore, the frequency of cyberattacks continues to rise, so if your business hasn't been hit yet, it more than likely will be.

Take the time now to prepare your technology and staff to discourage future intrusions, and educate your employees on how to quickly identify and respond to potential attacks.