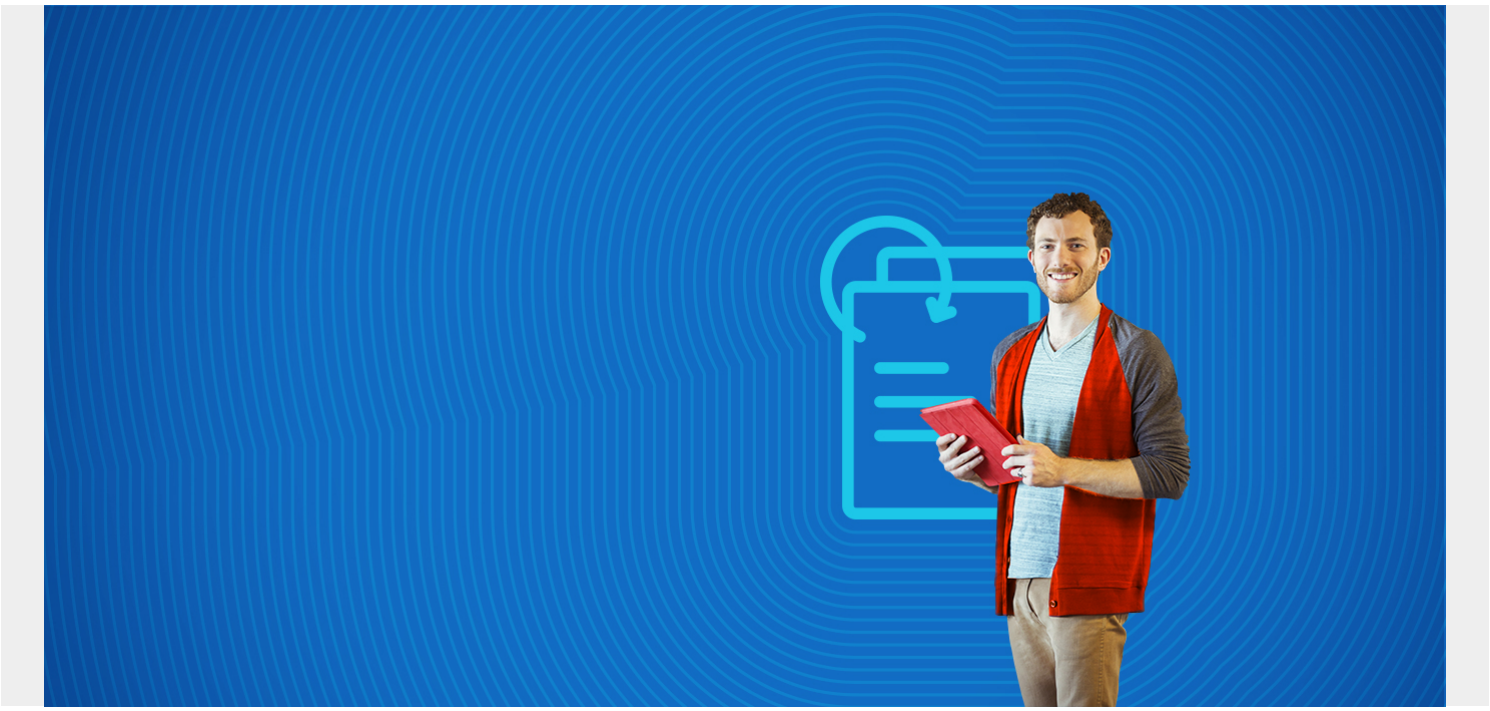
CYBERCRIME RISING: 6 STEPS TO PREPARE YOUR BUSINESS



You probably wouldn't think of leaving your house with the door unlocked, or even open. If you have an alarm, I imagine you set it each time you leave the house. Maybe you have a dog who you trust to warn of anything untoward happening at your home.

You protect your physical assets as a matter of course. But are you putting as much thought into protecting your business's digital assets?

Let's take a look at the current security challenges for any organization. Then, I'll share the six actions to take—regularly, often—to protect your data and your business as best as possible.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

Cybercrime & enterprise security

You probably think you are doing enough. But chances are that your enterprise is still at risk of attack from cyber criminals. This means that the information you safeguard for your customers is also exposed to the same dangers.

Every year we see:

- An increase in data breach events globally.
- Phishing attacks become more sophisticated and believable.
- Identity theft occurrences grow at a worrisome rate.
- Digital criminals come up with innovative ways to profit from any business with a digital presence that is not protecting itself adequately.

And this year proved that there's plenty more opportunity for cybercrime.

2020: A new world of criminal opportunity

The COVID-19 pandemic has caused many issues for businesses and individuals throughout the world. One group that has benefitted from the pandemic? Cyber criminals. As more and more people moved into remote working situations, businesses were unwittingly exposing themselves to increased vulnerability to incursion by cyber criminals.

Our new ways of working and shopping have created a perfect storm for those in our society who are willing to exploit security holes. As more and more retail transactions are conducted online there are greater opportunities for credit card data to be hacked. With workers moving to their home offices and connecting remotely to working environments, hackers have found new ways to exploit previously unknown security flaws.

Not only has there been a surge in the number of attacks—in the first quarter of 2020 cyber attacks against financial institutions were reported to have risen more than 230%. The techniques being used have improved and become harder to fight effectively. Hackers are using social engineering and increasingly advanced tactics to exploit:

- The human factor
- Weak links caused by processes and technologies in use by the supply chain

Luckily, there are steps you can take to increase your security, at least as much as possible.

Six steps to protect your business from cybercrime

Here's the bottom line: Every organization will always be exposed to risk. But these steps will help limit that risk.

1. Educate

More workers are connecting remotely to business systems. Proactively and routinely inform your employees about the ways criminals are likely to try to exploit their isolation to gain access to business systems.

Sophisticated and believable phishing attacks have increased exponentially and can be hard to spot, particularly when workers can't easily discuss suspect emails or messages with colleagues, as they would in the office. Regularly reminding your organization about phishing techniques will keep staff

alert.

2. Patch ASAP

Promptly applying security patches is more important than ever. New ways of working have exposed previously unnoticed security flaws and you can be certain that criminal elements will try to exploit these before enterprises have time to apply the appropriate patches.

Act swiftly to block these holes as soon as you identify them.

3. Block fake websites

Act quickly to block fake websites identified in phishing attacks. Previously, we were used to seeing phishing emails, often attempting to harvest login details for banks and financial institutions.

This year brings a new criminal opportunity: Many fake donation websites have been set up, targeting people who are willing to help others affected by the pandemic. Reports of company employees receiving emails, purportedly from their own CEO, directing them to fake charity sites have been reported.

Block these fake websites for your enterprise users, but don't stop there. Alert your national cybercrime agency of the fake websites as well.

4. Secure mobile devices

Ensure that mobile devices and other endpoints are adequately secured. With an increasing amount of business being conducted on tablets and smartphones, you must ensure that these, whether personal or organization-owned devices, are kept up to date with all applicable security patches.

Deny access to any unpatched devices that try to access company applications and networks. Create a policy for physically securing devices that can connect to company data—and ensure all staff agree and comply. Zero trust network access could be the way to do both.

5. Control all apps

Understand and control all applications in use in your organization. Many organizations saw an upsurge in the use of non-approved collaboration platforms as the result of the rapid move to home working—something known as shadow IT. The proliferation of these platforms was understandable, and in many cases essential to enable staff to remain productive.

With the dust now settled and a new normal being accepted, now is the time to review and rationalise the ways your teams collaborate internally and externally. Check the security credentials of all services in use and remove those that don't meet your requirements for security, privacy, and data integrity. A healthy and routine asset management practice will help you do this.

6. Review your SecOps practices

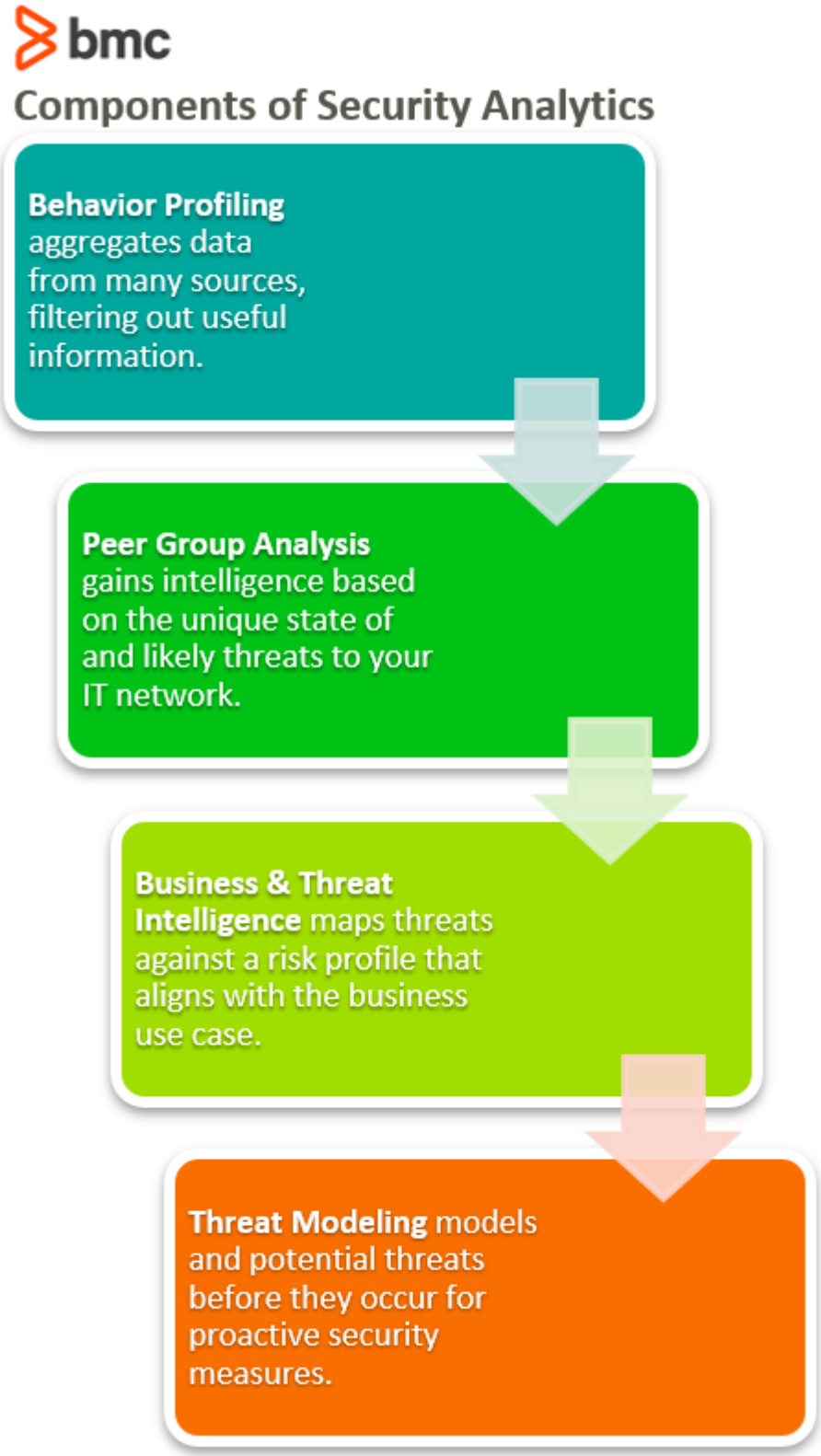
2020 has been a year of change. You need to make certain that the security and operations practices you have in place are adequate to:

- Keep your organizational data safe

- Protect you from incursion by the bad actors of the cyber world

I recommend these ongoing practices you can adopt to bolster security:

- Deploy automation that constantly checks the integrity of your systems.
- Conduct regular penetration testing so that you understand your vulnerabilities.
- Use the four components of security analytics.



Stay vigilant, stay aware

Protection against cybercrime is one area where organizations cannot afford to let down their guard. Recovering from cybercrime costs $200,000 on average, for companies of any size. Whether that's a sizable chunk of change or a drop in the bucket, there are better ways for you to invest your dollars.

Unfortunately, cybercrime protection is not a set and forget capability—criminals are constantly changing their methods, finding new ways to exploit your vulnerabilities, and harvesting your confidential data.

You must remain vigilant. Keep abreast of new methods of attack and protect your business from harm. The financial and reputational future of the organization depends on you.

Additional resources

For reading on related topics, explore these resources:

- BMC Security & Compliance Blog
- Risk Assessment vs Vulnerability Assessment: How To Use Both
- What is Security Orchestration, Automation, and Response (SOAR)?
- 8 Ways Hackers Will Exfiltrate Data from Your Mainframe
- Cybersecurity: A Beginner's Guide