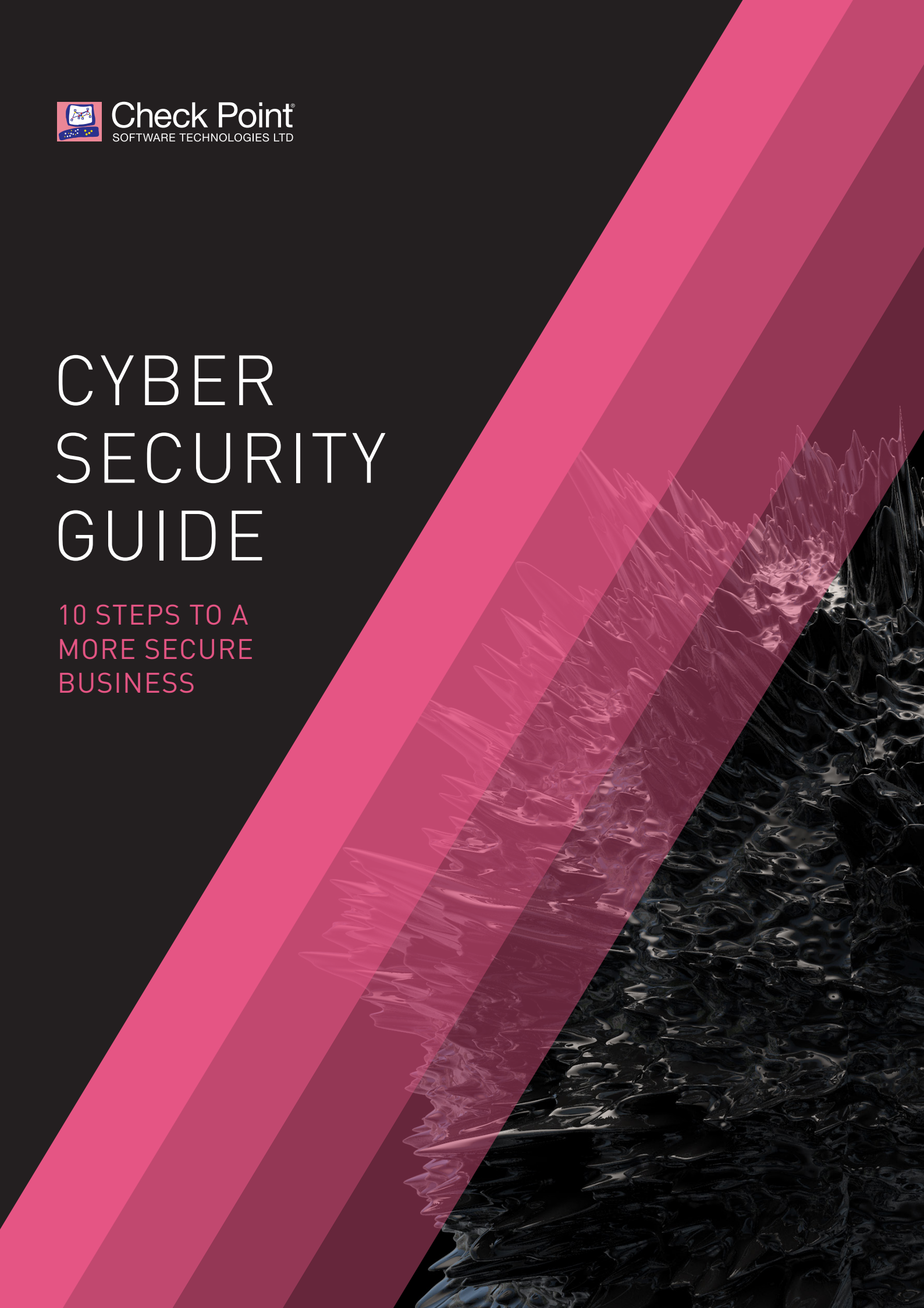
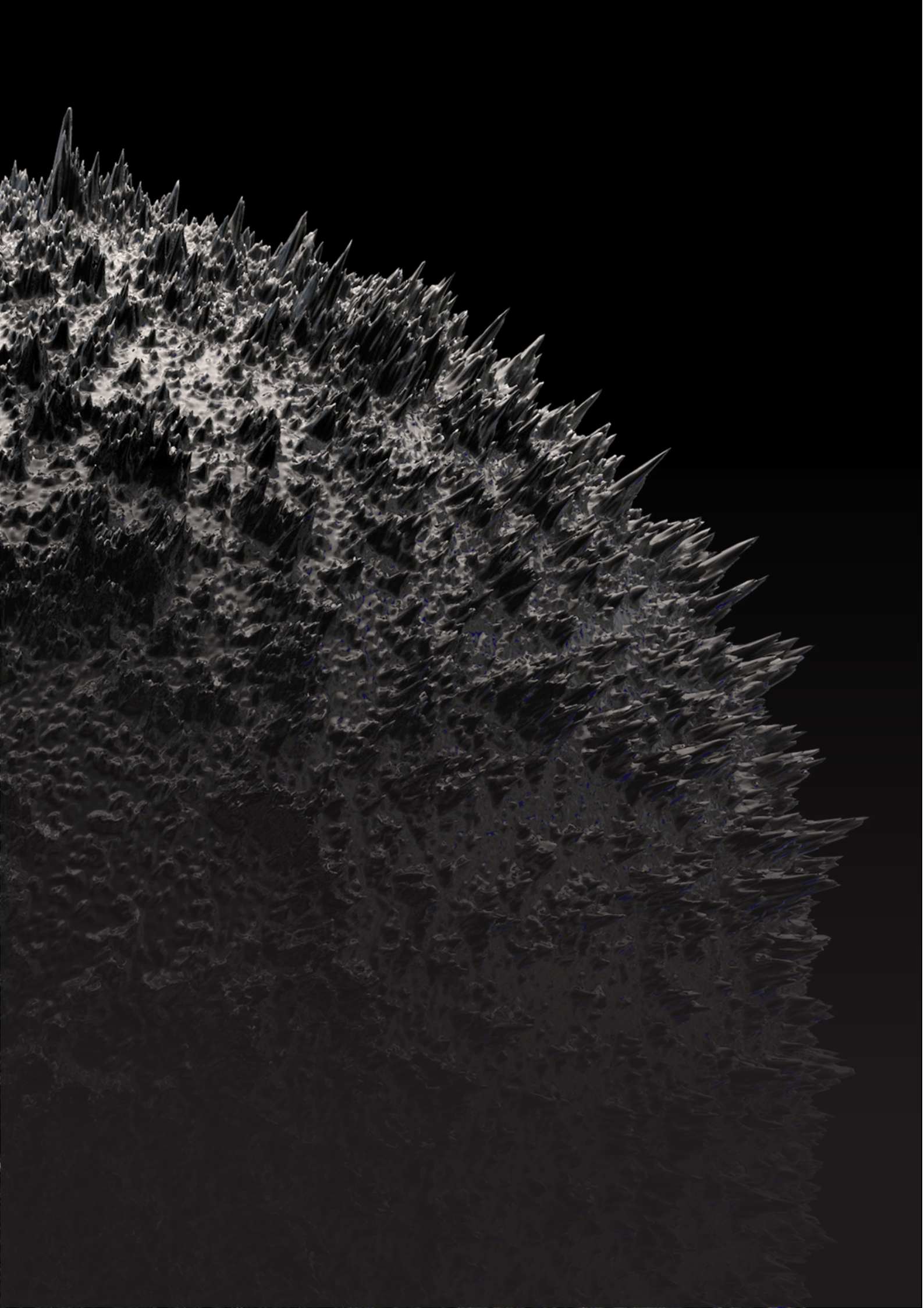
Check Point
SOFTWARE TECHNOLOGIES LTD

CYBER SECURITY GUIDE

10 STEPS TO A MORE SECURE BUSINESS





CYBER SECURITY GUIDE

10 STEPS TO A MORE SECURE BUSINESS

GETTING SERIOUS ABOUT SECURITY

FOREWORD

Just as we've learned to tune out car alarms, so have we become impervious to the headlines of cybercrime. That's despite cybercriminals stealing over 500 million identities[1] in 2014, alone. According to a December 2014 Computer Weekly article[2], "The production of malware continues on an industrial scale, with exploit kits and malware services putting sophisticated attack methods in the hands of relatively unskilled cyber criminals." And unfortunately, ignoring the issue will not make it go away.

Like it or not, businesses have the burden of protecting information with the same vigor as governments protect secrets. Whether your company's business is in technology, banking, healthcare, fitness, or fast food, if you sell something, chances are you have personal data stored in your network.

Network assets require the same round-the-clock protection as physical inventory or bank deposits. Some companies understand exactly how to accomplish this, while for others security is a mystery.

Understanding your exposure to threats — and what you can do about it is not only responsible business management — it's critical to business survival.

In the following pages, you'll find 10 steps to help you lead your organization to a more secure posture.

We want your business to grow, to flourish, and most of all, to be safe.

> THE PRODUCTION OF MALWARE CONTINUES ON AN INDUSTRIAL SCALE.

1 "Officials warn 500 million financial records hacked", USA Today, Oct 2014
2 "Top 10 Cybercrime Stories of 2014", Computer Weekly, Dec 2014

UNDERSTANDING THE NEED

Exposures and Access

Data risk is real

Cybercrime used to be an issue most people thought only governments dealt with. However, every year cybercrime strikes closer to home. In most cases, we are not even aware a threat exists until after it strikes.

In 2014, Target, Home Depot and Sony breaches made headlines. But if you weren't in the industry, you may not have heard about the thousands of other breaches from companies large and small, from every industry, relating to all kinds of data. While the 'smaller breaches' may not seem as impactful, each one provides data for more breaches, since most people make only minor modifications to passwords between their accounts.

The rule of 1 and 3

Information security risk is the combination of three factors: assets, vulnerabilities and threats (assets are exposed by vulnerabilities that may be exposed to threats). One breach becomes the seed for more breaches.

All three factors have risen during the last years. Here's why:

1. As the Internet becomes even more ubiquitous, with more of our lives intertwined with the web, we take for granted that our information and personal data are not at risk. As long as we limit our website access to legitimate businesses and don't give out our passwords, we're safe, right? Wrong.
2. The more comfortable we get with interacting and doing business online, the more digital footprints we leave — and that can lead to even more vulnerability.
3. Cybercrime has become an industry unto itself. The volume of threats has reached staggering proportions and continues to grow and evolve.

A Rand Study[3] asserts that cybercrime is in many instances more profitable than drug trafficking because it is easier to manage with fewer people resources, much lower risk of detection, and even lower risk of prosecution.

Addressing the problem

The explosive growth of threats has led to a new, heightened awareness — and actions to address the problem. Governments are weighing in, as are law enforcement agencies. It is time for companies to redouble their proactive security efforts.

3 Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar, Rand Corp, 2014

The more risk-aware businesses — from small to large — are seeing the need to bring security into sharp focus. It's not just about protecting, it's about enabling.

Over the years, companies have begun to learn they need to bring cyber security up to par with physical security. Physical break-ins require manpower and proximity; it is easier to inventory and track the losses. A cybercriminal, on the other hand, can break in from the other side of the globe in seconds. It can take weeks to figure out what they stole, not to mention how to track it back to the thieves. Moreover, cybercrime has a much bigger impact on most company's bottom line than physical crime.

Yet while most executives now rank cyber security about as high as physical security, they have been slow to bring it up at a Board meeting — until there is a breach. Thinking about security proactively needs to be the new order.

When a company is in the business of using or managing personal data, the ante is raised and legal regulations must be followed. Access must be policed and precautions need to be taken. Personal data needs to be treated as sensitive information.

As of 2014, the average value of an identity was priced at $188. While that may not seem like a lot, identity information is typically stored — and stolen — in batches of tens of thousands to millions at a time. That adds up to some pretty significant losses.

Access to sensitive information should be restricted to just those who need it. This way, you can track and trace any breach more efficiently. As a result, safeguards are easier to manage.

Assign responsibilities

The reason more people are not overly concerned about cybercrime is that they do not fully understand the implications. Most people do not appreciate that they could be out of a job if a cybercriminal steals their company's designs; or that stealing the online game login information allows hacking into bank accounts because cyber criminals know that many people reuse passwords across multiple accounts.

Proclaiming that protecting company information is everyone's responsibility is not enough. People need to be accountable at the individual level and made to feel invested in the company's security. And, security needs to be an embedded, planned part of the infrastructure — not an added-on afterthought.

Creating a culture of information security requires:

A. **Wrapping your mind around it.** Give careful consideration to how you want your company and your employees to operate. Then, create the culture that allows that vision to be realized, using security as an enabler.

B. **Looking ahead.** Know the required regulations and the threats and vulnerabilities. But don't forget to look at the big picture to map a security policy that will help you achieve that — not just now, but down the road.

C. **Minding the details.** Rally top management around the security policy and put it into action with clearly defined responsibilities.

Above all, don't overcomplicate things. When your security policy is simple and clear, you achieve a higher success rate with people adhering to your policy.

10 STEPS TO A MORE SECURE BUSINESS

A | WRAP YOUR MIND AROUND IT

B | LOOK AHEAD

C | MIND THE DETAILS

A. WRAP YOUR MIND AROUND IT

1 USE SECURITY TO UNLOCK INNOVATION

Security does not need to be the enemy of innovation. A robust security approach can do more than just protect the company from attack; it can also spur migration to more comprehensive foundational technologies that can advance your business. The value of striking the balance between risk assessment and the benefits of what new technologies can bring should not be underestimated. Often, innovation can both protect and increase performance.

When you adopt new innovative solutions and devices, a security risk assessment should be part of the vetting process. Take appropriate security measures into account as early as possible in the adoption period. As you look at your business needs, think through your infrastructure, what you want it to do, and how security can empower your objectives — before you build it out.

Be sure to engage a security expert with your IT planning so it becomes embedded and not simply bolted on. This gives you the deeper level of protection you need in order to unlock innovation.

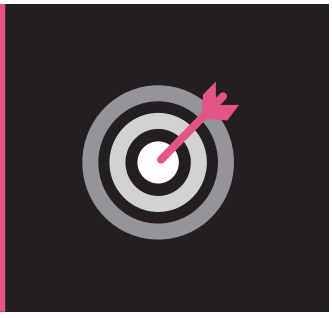
CONTINUED >

2 TEST THE LIMITS

One mistake some businesses make is to assume that once they implement security measures, the job is done. In today's world, that couldn't be farther from the truth. Threats are morphing and cybercriminals learn as they go, increasing their level of sophistication. Vigilance with regard to the threat landscape, along with enforcing your systems and policies, is critical.

Continuous assessment of your company's resilience against cyber threats and vulnerabilities helps measure the progress and adequacy of security activities. Test your infrastructure regularly with intrusion detection and on-the-spot audits. Consider working with third parties to identify vulnerabilities. Partner with industry peers and stay current on emerging threats.

3 STAY FOCUSED



With the volume of threats in today's world, managing your organization's IT security can be like trying to fix constantly springing leaks in a boat. The key is to understand the information or data that is most critical for keeping your business afloat.

Take a look at where your organization would be most vulnerable in the event of a security breach and make that your top priority. Consider issues like loss of confidential information, corporate reputation, noncompliance with regulations. Then, focus on what you can do to minimize the risk.

CONTINUED >

4 BE PREPARED

It's a motto that's held by the Boy Scouts and it should be held no less dear to anyone charged with securing the integrity and operations of a company. No matter how careful you are, security incidents will happen. In the current threat and vulnerability environment, you should not wonder "if" but rather "when" you will be a victim. How you handle that incident — more than the incident itself — can be a make-or-break moment. There is not one company breached in 2014 that expected to be a victim before the incident occurred. The ones that had a plan recovered the quickest and with the least negative impact.

Make it your business to have a disaster recovery plan. The larger and more complex the organization, the more types of incidents you should account for. Consult with a third-party expert to better understand and anticipate the possible threat scenarios. Identifying them in advance will significantly reduce response times in case of an actual breach.

Take charge with your responsiveness and remember that communication is key. Those who shrug off the importance of that rule find themselves inundated with unwanted attention when their security hits the skids.

Have a well thought out communications plan in place in the event of a security incident, with discrete, relevant messaging for internal audiences, external audiences, and authorities as needed.

B. LOOK AHEAD

5 SEE THE FOREST

When thinking through your security posture, it's important to see the threats and vulnerabilities. But it's also critical to see contributing factors and the big picture of where you're trying to lead your organization.

According to a 2014 Security Services report from IBM[4], over 95% of all incidents investigated cited human error as a contributing factor. While some of the errors were from system misconfiguration and poor patch management, the report also pointed to lost laptops or mobile devices, disclosure of regulated (sensitive) information via incorrect email addresses, or opening infected attachments/URLs listed among the top five reported infection incidents.

Ultimately, security is everyone's problem in the organization. The most prepared businesses know that security policy needs to stem from strategic goals, business objectives, and corporate policy — and tie to procedures and requirements, performance measurements, and of course, people at all levels of the organization.

If you want a healthy forest, you need to tend to the ecosystem that surrounds it.

Educate people on how risk can be minimized and how strong security can advance business, versus hamper it.

4 IBM Security Services 2014 Cyber Security Intelligence Index report

CONTINUED >

6 PUSH BEYOND ADEQUATE

Security compliance is, among other things, on the long list of laws and regulations by which companies must abide. Unfortunately, many believe that if they meet the requirements governing privacy, finance, and consumer protections, they're covered. But this kind of thinking can trim the scope and effectiveness of good security posture. Compliance is typically focused on specific threats, making it less comprehensive than a security posture could and should be. Since it does not ensure a secure network, it shouldn't be the basis of your policy. So with that in mind, push beyond compliance. Create strong security policy that safeguards information and supports response mitigation. Then, build compliance into that.

7 MAKE IT OFFICIAL

Making corporate information security policies official — and sharing companywide — can yield some pretty powerful benefits:

- You create a standard across the company for all employees to reference, which becomes part of the culture
- More people become invested in and committed to protecting vital information assets; and
- Your exposure to threats becomes more manageable

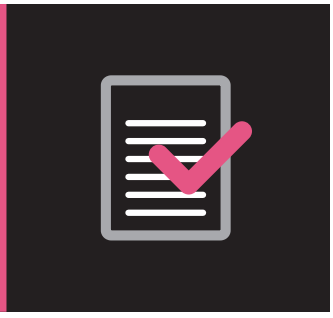
When you engage a larger population to help you implement policy, enforcement becomes more efficient. For instance, on average, there is one police officer per 600 residents in cities with population sizes over 50,000. When the general public is engaged in complying with the law, citizens obey the rules.

It works the same way in business. Involve your workforce in improving your information security posture by educating them on how they can help. Create information security policies that employees can understand and help reinforce.

C. MIND THE DETAILS >

C. MIND THE DETAILS

8 GET BUY IN



Global objectives have the greatest impact when they come from the top. And, protection of your organization's information must be a global objective. For many executive managers, information security is not at the top of the priority list; you have to get it there.

Breaches during the past five years across almost every industry provide plenty of data on the potential downside of not making security a priority. Find examples of companies similar to yours and highlight the potential risks to your management. If they are not already onboard, providing data should help get them there. Securing adequate resources — in terms of both financial budgets and people — is important for the protection of the company. Executive signature of the company security policy demonstrates active support.

Help everyone — from top down — understand the importance of mitigating cyber-related risks to protect intellectual property. This, alone, safeguards the heart of the company and helps it maintain competitive advantage.

Since we all know that numbers and data speak louder than words, establish a measurement system that lets you report regularly on your information security progress. In addition, make sure you share metrics with top management at least once a year.

You'll want to identify key security indicators and chart the effectiveness of the security measures in place. This offers valuable insight for ongoing optimization of your security policy, as well as for future investment in security.

9 CREATE ACCOUNTABILITY

Managing information security in an effective and efficient manner requires tools, training and methods of measurement. And, since employees sometimes see enforcement as a negative, it also requires good internal communication. It is vital to make sure methods, measurement techniques, and security initiatives are shared and explained. Let your teams know about the latest threats, and investments the company is making to provide overall protection.

Train staff to help them understand how they're accountable and what their roles are in helping to protect against threats. An especially important topic to focus on is social engineering, because of its prevalence.

Regardless of your company's size, have your employees take a quiz on your security policy to reinforce its importance.

For larger companies, take the time and thought to identify specific individuals who will be the stewards of your information security policy. Distinct responsibilities should be mapped out for each person, along with a clear understanding of how individuals intersect. Document and share this information so everyone involved is in the know.

Don't forget to go beyond your walls to share information with others in your industry. This can be an invaluable network when it comes to identifying best practices and averting upcoming attacks.

CONTINUED >

10 NEVER EASE UP

For some businesses, security management is outsourced due to lack of resources or expertise. Often, services like backup-and-restore and encryption, and data protection can be especially attractive to small businesses. But outsourcing comes with its own risks.

External companies that are not adequately protecting information or information systems may pose a serious liability to an organization's business operations, reputation and brand value.

Here are some guidelines to keep in mind:

1. Require your service providers or suppliers to follow your information security policies.
2. Make sure service level agreements (SLAs) are defined and adhered to, and include specifics around system availability and restoration metrics. Periodically audit to make sure your service provider is meeting the SLA. Check their activity logs to analyze and evaluate threats.
3. Keep in mind that when it comes to cloud services, there are special information security policies. If you're working with a service provider to store, process, or manage data on a network, familiarize yourself with their policies and what is covered.

Whether IT service providers, cloud providers, or an outsource company, if they have access to, or manage any data critical to your company's operation, make sure you understand their security policies and safeguards.

CONCLUSION

TURN SECURITY INTO AN ENABLER

Given that data is the cornerstone of businesses, today's leaders cannot afford to ignore security. Without proper policy, both customers and the company, itself, are put at risk. By understanding potential threats and vulnerabilities; creating a solid plan that aligns with your business; and ensuring protections are integrated into your IT infrastructure, you can turn security into an enabler, rather than a disabler.

Take a proactive step to ensure your organization is secure. Sign up for **CHECK POINT'S SECURITY CHECKUP** — a free onsite assessment that can uncover potential risks to your network:

http://www.checkpoint.com/campaigns/securitycheckup/index.html

Check Point®
SOFTWARE TECHNOLOGIES LTD

WE SECURE THE FUTURE

To learn more about how to secure your organization,
please visit www.checkpoint.com

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

January 2015