Microsoft

The Modern Workplace Watchdog

Protecting the information, systems, and people important to you and your business

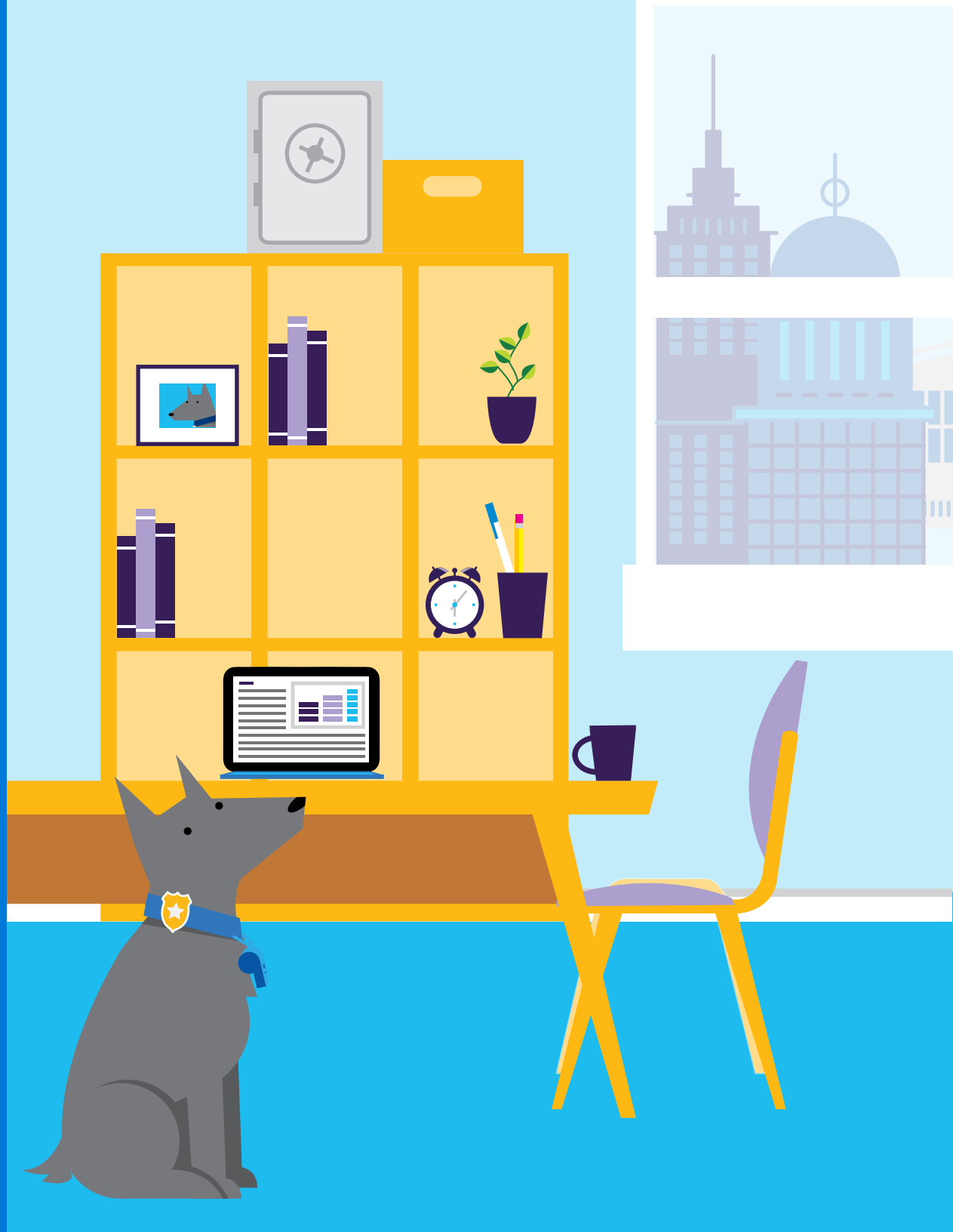


TABLE OF CONTENTS

The Times, They Are A-Changin'

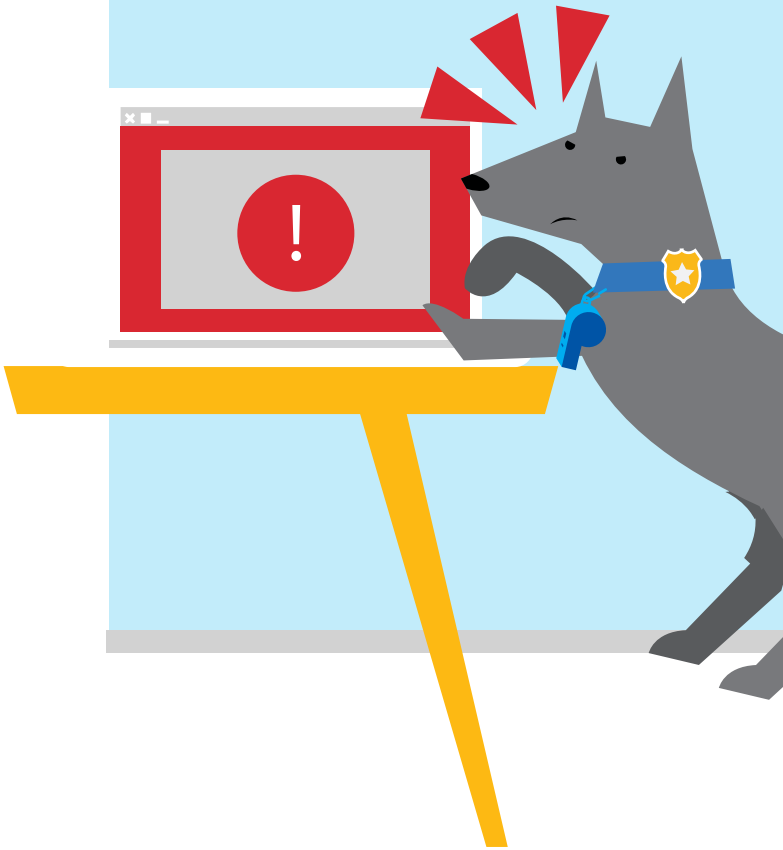
The Times, They Are A-Changin'

Today's businesses are fighting an uphill battle against an enemy that is adapting at an alarming pace. This enemy, the modern computer hacker, looks to exploit weaknesses in your business's software infrastructure and extract valuable information for personal or political gain. Computer hackers can take many forms—whether they're a highly trained network of "hacktivists" like Anonymous, or a teenager who acts alone and learns from online tutorials.[1] Motivations for cyber attacks vary, but one thing is for sure: in the current cybersecurity landscape, nobody and no business is immune to the threat of hackers.

In 2014, 47% of Americans had their personal information stolen by hackers, mostly through data breaches at large companies.[2] New reports from the Internet security teams at Symantec and Verizon revealed that more than 317 million pieces of malware were created last year—that's nearly one million new threats released every day.[3] The report also shows that directed attacks and data breaches increased by 40% from 2013 to 2014, with five out of six large companies having been targeted by cybercriminals.

In spite of these statistics, there is good news. By reevaluating their cyber defense strategies and investing in the latest technology, today's businesses can remain resilient amidst the changing risks they are facing. Combining a modern security strategy with updated technology can significantly help raise the bar on would-be attackers and reduce their potential return on investment (ROI).

In this eBook, you'll get an overview of the current cybersecurity landscape, discover how a renewed focus on basic security hygiene—including keeping your operating system up to date—can bolster your organization's cyber defense, and learn how to implement a strategy that protect your company's identities, devices, and data from today's threats.



1 Boy, 16, bailed over TalkTalk hacking attack - BBC News. (2015, November 4).
2 These Cybercrime Statistics Will Make You Think Twice About Your Password: Where's the CSI Cyber team when you need them? - CBS.com. (2015, March 3).
3 Harrison, V., & Pagliery, J. (2015, April 14). Nearly 1 million new malware threats released every day. Retrieved November 17, 2015, from http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

Chapter 1

The Dark Web

The Dark Web

There are portions of the World Wide Web that you won't find through any traditional search engine. In fact, the only way to access these portions of the Internet are by using special tools that ensure anonymity and make visitors virtually untraceable.[4] This hidden network of websites is often referred to as the "dark web" and serves as a digital black market for hackers to buy and sell high-value data assets stolen from individuals and businesses. It is on this shadowy corner of the Internet where hackers dumped 15G worth of information on crowdfunding service Patreon's users earlier this year, including their names, emails, and posts. It is also where hackers released the personal information of millions of federal employees, their friends and family members after they infiltrated the server at the Office of Personnel Management.

According to a recent study by the RAND Corporation's National Security and Research Division, the "dark web" has emerged as a "playground of financially-driven, highly organized, and sophisticated groups," and in certain respects, the black market for stolen data can be more profitable than the illegal drug trade.[5] The study notes that the increasing size and complexity of the hacker market poses a formidable challenge and severe threat to businesses, governments, and individuals operating in the digital world.

"Between November 2014 and June 2014, Microsoft tracked about **1,700** distinct website credential thefts, comprising a little more than **2.3 million** credentials that were posted in public places on the Internet.[6]"

4 Lee, A. (2015, August 19). What You Should Know About The "Dark Web," An Anonymous Haven For Hackers.

5 Ablon, Lillian, Martin C. Libicki and Andrea A. Golay. Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Santa Monica, CA: RAND Corporation, 2014. http://www.rand.org/pubs/research_reports/RR610.

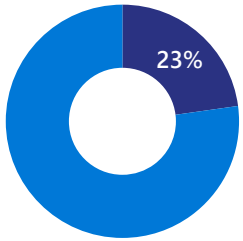
6 https://blogs.microsoft.com/cybertrust/2015/07/20/cloud-security-controls-series-multi-factor-authentication/

The Dark Web

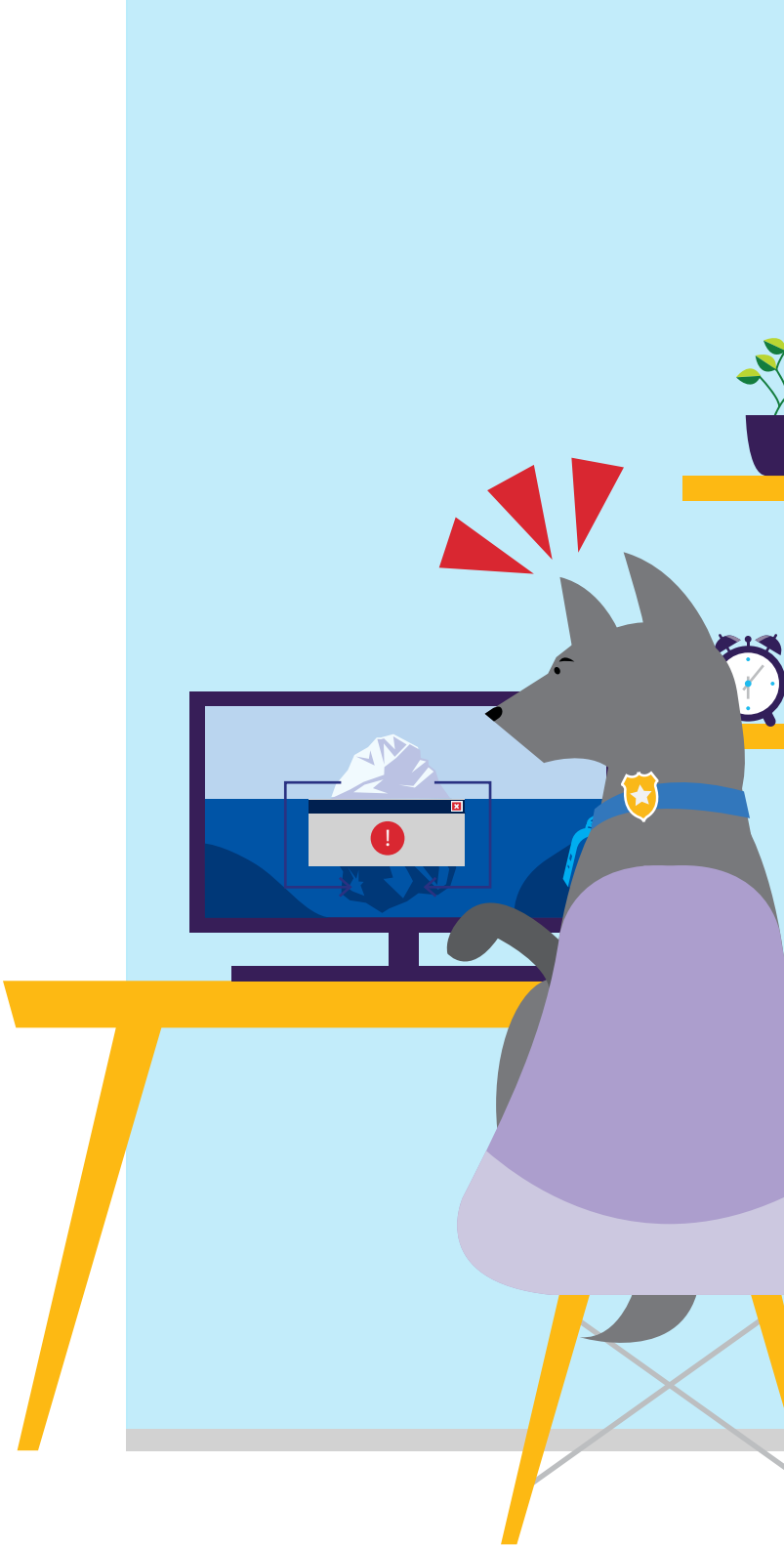
Quantifying the economic impact of data breaches on businesses is tricky, but there are some statistics available. According to the Ponemon Institute, the per-record cost of a data breach reached $154 this year, up 12% from last year's $145.[7] At first glance, that may not seem like much, but consider that the average data breach results in 10,000 stolen records—and don't forget to factor in related costs like damage to corporate reputation, loss of customers, and business interruption. Overall, the average total cost of a single data breach increased 23% from 2014-2015 to $3.79 million.

With the proper cyber defense strategy in place, your business can safeguard against cyber attacks and the unwanted costs that occur as a result of being hacked.

The per-record cost of a data breach reached $154 this year, up 12% from last year's $145



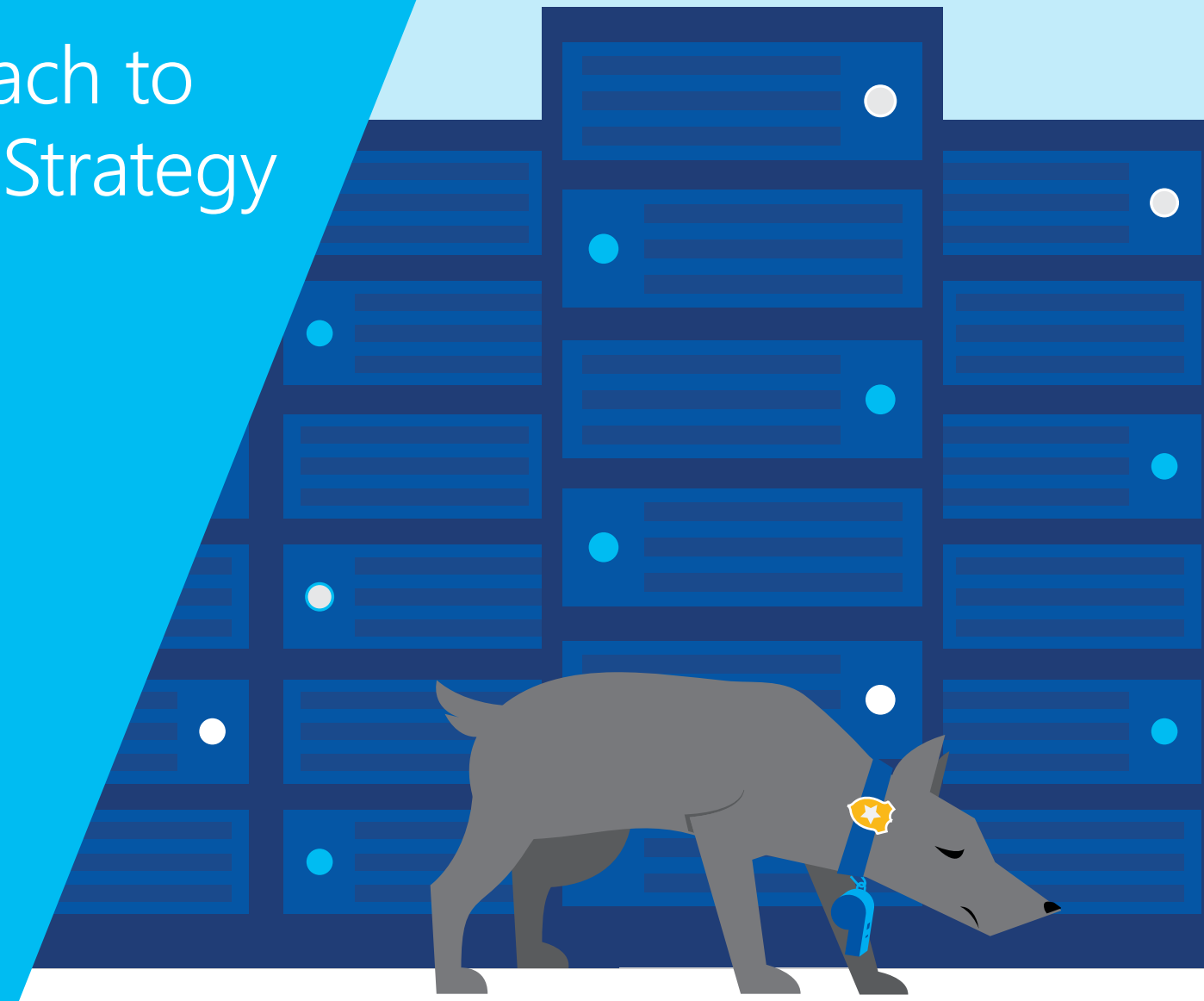
The average total cost of a single data breach increased 23% from 2014-2015 to $3.79 million.



7 Korolov, M. (2015, May 27). Ponemon: Data breach costs now average $154 per record.

Chapter 2

A New Approach to Cybersecurity Strategy



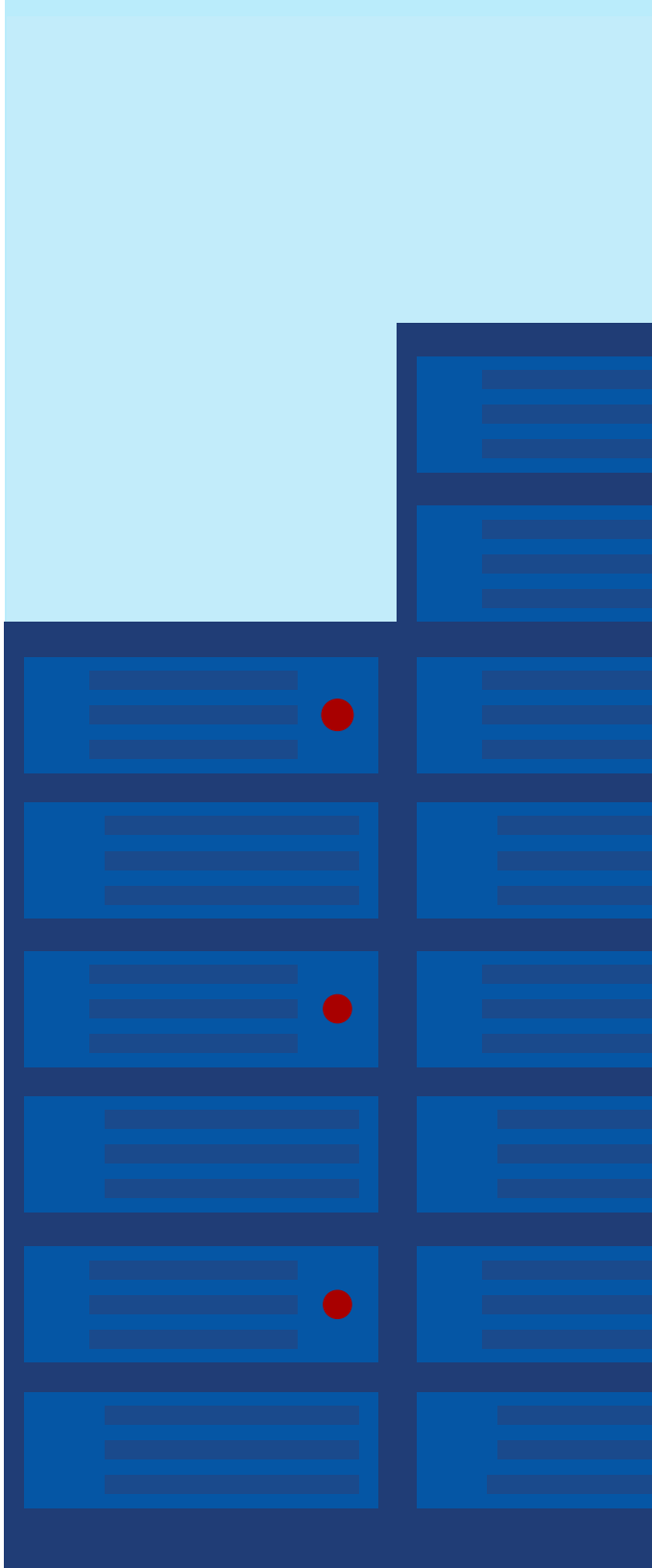
A New Approach to Cybersecurity Strategy

According to KPMG's Global CEO Outlook 2015 report, a whopping 50% of CEOs polled indicated that their firms are either not prepared, or only partially prepared, to deal with a major cyber event.[8] Today, an alarming number of businesses are employing an old-fashioned security strategy that no longer works in the current cybersecurity landscape. This "protect and recover" strategy operates under the unrealistic assumption that if your business protects well enough, it will never get breached. As we've seen in recent years, however, no individual, business, or government is immune to the threat of data breaches as the cybersecurity landscape continues to evolve and attacks become more sophisticated.

Rather than focusing on a purely preventative strategy, Tim Rains, Chief Security Advisor of Microsoft's Enterprise Cybersecurity Group, and other cybersecurity experts at Microsoft recommend businesses adopt a more holistic approach to cybersecurity. This holistic approach, also called an "assumed breach" strategy, has three components:

- **Protection**
- **Detection**
- **Response**

This new, holistic security posture emphasizes breach detection, incident response, and effective recovery. By investing in what would happen in the event of a data breach and implementing controls and protocols that detect attacks and contain malicious activity, businesses can be equipped to be proactive and resilient about cybersecurity, and respond faster to cyber attacks. In a world where it is not a matter of if your business will get hacked, but when, a holistic cyber defense strategy can be among the most realistic and effective way to approach cybersecurity.



8 Steinberg, J. (2015, September 4). This Latest Cybersecurity News Should Worry You.

Chapter 3

Back to Security Basics

Back to Security Basics

Today, many breaches result from organizations stumbling on or neglecting basic security practices. According to Tim Rains, the overwhelming majority of data breaches happen in one of four ways:

- **Unpatched vulnerabilities**—Attackers locate a flaw, glitch, or weakness in your business's software or operating systems (OS) where security updates are available but are not deployed, and create exploits to target those vulnerabilities.
- **Misconfigured systems**—A web server, application, or plug-in has been misconfigured in a way that inadvertently leaks information or allows hackers an entry point into your business's software or OS.
- **Weak passwords**—Single points of verifications like passwords are bad news and can easily be bypassed by savvy hackers (more on this in Chapter 4).
- **Social engineering**—Hackers manipulate employees into installing malware on their own systems. This is the most common way people and businesses get compromised (more on this in Chapter 6).

A renewed focus on basic computer hygiene can help businesses be prepared for 98% of what hackers are doing today. Part of returning to security basics involves making sure your business is using an up-to-date OS that significantly raises the technical bar on attackers and reduces their ROI. Antivirus software, firewalls, and regular security awareness training can also safeguard your business against cyber threats.

If your business is running Windows 7 or 8, another easy way to up your cybersecurity game is to turn on Unified Extensible Firmware Interface (UEFI). UEFI is a standard firmware interface for PCs designed to protect your computer against attacks during the pre-boot process. It offers a modern security approach over the BIOS (basic input/output system) that has been a staple of PC design for more than 30 years.

Don't be so hyperfocused on the one to two percent of cyber attacks on the outside of the cybersecurity bell curve that you forget to focus on the basics.

"**Newer is better:** Running the latest version of document parsers, the latest service packs and security updates helps protect against [poor system hygiene] attacks.[9]"

9 Hall, A. (2014, November 18). 7 Precautions For Protecting Against Perpetrators. Retrieved December 21, 2015, from https://blogs.microsoft.com/cybertrust/2014/11/18/precautions-protecting-v-perps/

Chapter 4

Guard Your Devices

Guard Your Devices

Passwords are dead. They certainly had a good run, though. If you ask experts like Tim Rains and other security officials, they'll tell you that single points of verification like passwords no longer cut it in the current cybersecurity environment.[10] It doesn't matter if you train your employees to replace all of the "favorite pet" and "first child's name" passwords with unique and complicated alternatives. Even if the dictionary can't find your employees' passwords, savvy hackers can—and will. In August 2014, a Milwaukee, Wisconsin-based cybersecurity firm uncovered an estimated 1.2 billion stolen Internet logins and passwords amassed by a Russian crime ring from a series of attacks on more than 420,000 websites.[11]

It is now a necessity for businesses to have more than one layer of authentication to keep hackers out and ensure the only users on their networks are the ones who are supposed to be there. Two-factor authentication, or multi-factor authentication, is now a standard security feature of most operating systems that safeguards against "Pass the Hash" attacks and makes it much more difficult for hackers to access valuable information and assets. Microsoft Passport and Windows Hello* (more on these in Chapter 7) are two components of a flexible two-factor authentication solution that is offered on the latest iteration of Windows (Windows 10). By replacing passwords with an enrolled device (PC or mobile phone) and a biometric or PIN, these features combine to offer users enterprise grade authentication.

If your business is using an outdated OS without two-factor authentication, you are leaving your network vulnerable to potential data breaches that can easily be avoided.

"When an organization requires its employees to provide more than one factor in order to grant access to their data, it gets **more difficult** for a criminal to impersonate that employee. A stolen password on its own is no longer enough to gain access, and without the additional required physical element, a cybercriminal will be further challenged."[12]

10 Boyd, A. (2015, October 27). The 6 types of cyberattacks and top 5 defenses.

11 Finkle, J. (2014, August 5). REPORT: Russian Hackers Stole 1.2 Billion Internet Credentials. Retrieved November 17, 2015, from http://www.huffingtonpost.com/2014/08/05/russian-hackers-stolen-credentials_n_5652812.html

12 Hall, A. (2014, September 16). Cybercrime, Data Protection, and Multi-Factor Authentication (MFA). Retrieved January 18, 2016, from https://blogs.microsoft.com/cybertrust/2014/09/16/cybercrime-data-protection-and-multi-factor-authentication-mfa/

Chapter 5

Defend Your Data

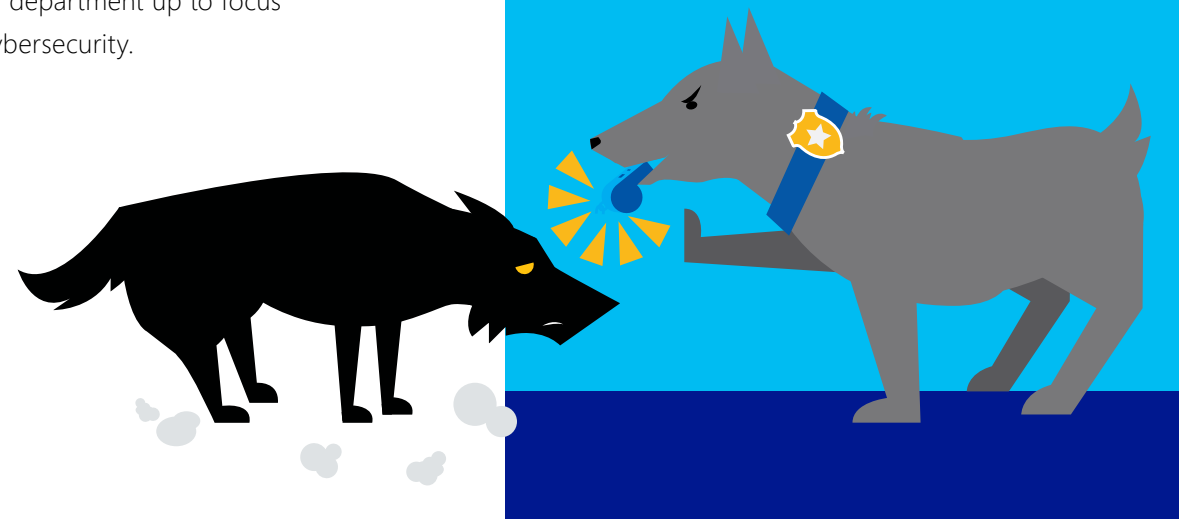
Defend Your Data

In our increasingly mobile and hyperconnected world, it is becoming more common for employees to use their personal devices to work on corporate projects. Whether employees are bringing their personal devices to work as part of a BYOD program or working remotely, there is an increased risk of accidental data disclosure any time individuals move between enterprise and personal apps. While BYOD is causing security issues, however, many data breaches actually take place in on-premise storage sites. To help ensure your both on and off premise, consider utilizing cloud computing.

In the first installment of The Modern Workplace Watchdog series, we mentioned that experts estimate 60% of businesspeople will be working in the cloud by 2022. Incorporating cloud computing into your business's security strategy allows for unprecedented agility by enabling employees to access a large store of corporate information from nearly anywhere at any time on their personal device. But because of the sensitive nature of this data, many business leaders worry that cloud computing will increase their vulnerability to hackers and other threats. In actuality, cloud computing can help businesses maintain the sturdy security and credential management of their business's network.[13]

Additionally, if an employee happens to lose his or her personal device or accesses a personal app that has the potential to inadvertently leak sensitive information, the cloud can allow IT departments to react promptly and address the security issue.

As part of a larger, holistic cybersecurity strategy, cloud computing can help your business be proactive about protection and free your IT department up to focus on client-side cybersecurity.



13 Shue, C., & Lagesse, B. (n.d.). Embracing the Cloud for Better Cyber Security.

Chapter 6

Protect Your Identity

Protect Your Identity

An earlier chapter briefly mentioned that social engineering is the most common way businesses and individuals get hacked. Rather than search for glitches and vulnerabilities in the framework of your business's network, social engineering involves hackers tricking individual employees into installing malware on their own devices. It is less of a technical approach to hacking and more like a psychological approach that isolates and manipulates a human being into granting cyber criminals access to their credentials.[14] Once a hacker has access to an employee's identity, he or she can freely roam around the network and snoop for valuable information.

Because social engineering attacks can take many forms, it can be extremely difficult to know who and what to trust when navigating the Internet. Often, savvy social engineers will disguise malware or other malicious software as legitimate-looking emails, plug-ins, and hyperlinks. For instance, an employee who wants to watch a video of cats playing the piano during his or her lunch break may be prompted to install a plug-in before he or she can access the video. Is this a legitimate plug-in or a hacker's attempt to steal credentials and get inside your business network? Security awareness and proper training can help prevent social engineering attacks by showing employees how to identify the difference between the two and think before they click.

Making sure your business is employing the most up-to-date OS and security software can also safeguard against social engineering attacks. To that end, we'd like to highlight some important features of Windows 10 that provide your organization with the security it needs to combat today's threats. The final chapter will provide an overview of these new and improved cybersecurity solutions. For a more in-depth discussion about what Windows 10 can offer your business, we suggest contacting your Microsoft account representative.

"Latest data shows **newer** versions of Windows have **lower** malware infection rates than older versions.[15]"

14 Goodchild, J. (2012, December 20). Social Engineering: The Basics.

15 Rains, T. (2015, May 19). Latest data shows newer versions of Windows have lower malware infection rates than older versions. Retrieved December 21, 2015, from https://blogs.microsoft.com/cybertrust/2015/05/19/latest-data-shows-newer-versions-of-windows-have-lower-malware-infection-rates-than-older-versions/

Chapter 7

Make Security a Priority for Your Business

Make Security a Priority for Your Business

The current perimeter-less, constantly evolving cybersecurity landscape is scary. Hackers are getting more sophisticated and organized. Attacks are getting more targeted by the day, week, and month, and can come from anywhere. But, hopefully you now know that safeguarding your business against the overwhelming majority of cyber attacks is not as daunting or time consuming as you might have thought. It is as simple as focusing on basic computer hygiene and not neglecting security 101 best practices.

If your business is using an outdated version of Windows or another OS, for instance, you are missing out on an easy opportunity to significantly up your cybersecurity game. Consider upgrading to an OS that has the bark and the bite to help protect the information, systems, and people important to your business. To evaluate whether or not your OS is built to handle the modern cybersecurity landscape and the unique challenges that come along with it, consider the following features:

- Two-factor (or multi-factor) authentication
- The most advanced antivirus and malware protection/detection
- Protection against accidental data leakage when moving between enterprise and personal apps
- Tamper-resistant hardware and software that safeguards your devices

Make Security a Priority for Your Business

With a host of new and improved features, Windows 10 significantly raises the technical bar on would-be cyber attackers and drastically reduces their ROI. Windows is updated one billion times per month for security purposes to address evolving security and compliance standards.[16] It runs the world's largest anti-malware, antivirus service. Additionally, Windows 10 contains the following features to help ensure your business network remains secure and vibrant:

- **Device Guard**—A combination of enterprise-related hardware and software security features that, when configured together, will lock a device down so that it can only run trusted applications.
- **Credential Guard**—Secures domain credentials using the virtualization-based security and block the credential theft attack techniques and tools used in many targeted attacks.
- **Windows Hello**—Offers users a more personal and secure way to sign into their devices with fingerprint ID, facial recognition, and PINs
- **Windows Defender**—Built-in malware protection that identifies and removes viruses, spyware, and other malicious software.
- **Enterprise Data Protection**—Protects sensitive data on enterprise and personal devices and safeguards against unintended or malicious use.
- **Microsoft Passport**—Works with Windows Hello to replace passwords with strong two-factor authentication that consists of an enrolled device and a PIN.

Microsoft has worked diligently to make Windows 10 the most trusted and secure Windows ever[17] – an OS that can help your business stay ahead of the cybersecurity and innovation curves. As part of a larger, holistic approach, running Windows 10 can bolster your business's defense and allow you to focus on other important tasks like driving technology forward and increasing productivity.

Over 200 million systems have upgraded to Windows 10 since its launch in August 2015. To learn more about how the new features of Windows 10 can help your business be more secure and productive, visit https://aka.ms/windowsfeatures.

Have questions about Windows for business? Request a contact from a Microsoft representative.

16 http://news.microsoft.com/security2015/
17 https://www.microsoft.com/en-us/windows/features

microsoft.com