Microsoft

Dark Corners

Uncovering the Risks of Cybercrime

piracy

n. The illegal duplication, creation and sale of unlicensed digital media

malware

n. software that is intended to damage or disable computers and computer systems

What is **CYBERCRIME?**

You built your business from the ground up, and are committed to its success. You even installed a security system to protect it. But did you know that every day your business is at risk from being attacked by cybercriminals, and you may not be protected?

That's because cybercriminals often operate in the shadows. These are usually nameless, faceless people and entities out to do you harm, steal your identity and confidential data and gain from your personal or business loss. While the effects of traditional crimes – breaking and entering, theft, etc. – are visible, cybercrime is often less noticeable and yet just as damaging to your business.

Cybercrime is generally considered to have two main segments, piracy – the illegal duplication, creation and sale of unlicensed digital media – or malware software attacks, both of which are often backed by organized crime. In this eGuide, we'll provide a summary of the two cyber-crime categories and explain the wide range of IT threats businesses and consumers face. More importantly, we'll share tips and resources you can use to stay informed, and ultimately, protect yourself and your digital assets – including three simple tips you can take right away.

Dissecting **DIGITAL PIRACY**

Today, the only thing digital pirates need is a keyboard and high-speed Internet connection. Digital piracy is considered one of the most visible forms of cybercrime, and you've likely seen it highlighted in government warnings at the start of movies and called out in packaging for CDs and DVDs. Most notably, digital piracy was a media boom in the late 90s and early 2000s. Remember Napster? The recording industry began a massive crack down on illegal downloads. And in 2001, the Recording Industry Association of America successfully prosecuted the popular file sharing service for facilitating the illegal downloading and uploading of copyrighted music[1]

Despite existing before the dawn of the Internet, the ease of access and global reach of the Web has led to an explosion in digital piracy. Today, cybercriminals can operate globally, setting up a virtual storefront and allowing users to purchase and download stolen content anytime, anywhere. However, downloading pirated files goes well beyond the lost revenue experienced by the content creator.

Imagine you're a business owner looking to upgrade to Microsoft's latest operating system. Your local computer store is selling an upgrade for $100, but you found the same software online for $40 from an unknown vendor. Feeling as though you've hit the jackpot, you whip out your credit card to purchase the discounted software – which also comes with malware on it! Unfortunately, because of the malware, you might also be providing your credit card information and access to your computer network to an organized crime syndicate in Eastern Europe. In fact, in its recent report, The Link between Pirated Software and Cybersecurity Breaches, IDC found that malware in pirated software can be a lucrative venture, with an organized crime ring Microsoft helped uncover earning more than $2.2 million in revenue every day.

The Other Side of **CYBERCRIME**

Now, let's discuss malware. While piracy gets the most air time, an equally important and potentially more harmful side is that of malware. Often, these forms of cybercrime coexist with piracy, using illegal digital downloads as the vehicle to infect users' machines. In its simplest definition, malware is harmful software – this may include viruses, spyware, ransomeware or Trojans designed to damage or disrupt a computer system. Others, can be complex programs designed to disrupt your network services or steal private data, developed by sophisticated and well-funded organized crime rings.

While reputable business owners likely avoid buying Microsoft Windows from a person standing on the corner of a street, the Internet has made it easier for criminals to hide their true identity to unsuspecting buyers. Cost-conscience shoppers are increasingly turning to the Internet to find better deals. In its Total Retail: Global survey of online shoppers report, PwC found that 55 percent of respondents shop online due to lower prices. Unsuspecting shoppers can then fall prey to the trap set by cybercriminals, unknowingly purchasing counterfeit software in their bid to find the best deal. These crimes are not as well known or publicized as piracy.

With a majority of users feeling they are more protected than they really are, businesses and consumers alike unintentionally increase their risk and create a more inviting digital environment for sophisticate cybercriminals.

Oftentimes, these networks of criminals are a much more structured operation than many cybercriminals. Crime syndicates creating elaborate online storefronts may be using the proceeds to fund other illegal activities while embedding malware into the software, putting sensitive financial and customer data at risk, without the user's knowledge.

Businesses, Consumers and the **NEW LINE**

Cybercriminals target both consumers and businesses, with personal devices brought into the workplace blurring that line. However, the methods they employ, their end goals, and how they commit their crimes can vary greatly dependent on their ultimate target.

Own a small businesses? Cybercriminals are more likely to target you due to lower security protections and lack of dedicated IT personnel. Consumers, meanwhile, can find themselves targets of identity theft or have their PC turned into a botnet providing computing power to support more intensive online attacks.

One of the easiest ways for cybercriminals to target businesses and consumers is through the use of pirated software. Not only will buyers find the software or device unsupported by manufacturers, they have a 33 percent chance of encountering malware bundled within, according to IDC. Users in North America also find themselves increasingly at risk of being targeted by cybercriminals. In fact, IDC's research found that while North America has the lowest piracy rate among all regions studied, an estimated 24 percent of network outages are caused by cybercriminals – leading to the highest per record costs from data breaches.

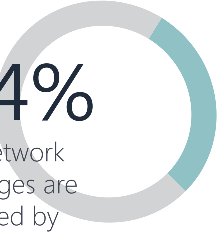
Businesses have a lot to lose from cybercrime, with victims finding themselves addressing three key issues – computer security, data loss and damages to their reputation. And, the line between business and consumer is being blurred by the increasing use of bring-your-own-device (BYOD) policies, with IDC researchers noting consumers are generally more likely to use pirated software than enterprises, even bringing it to work. With more than half (58 percent) of end-user PCs having no effective software audits, increasing the likelihood of infection.

And these infections can lead to extensive costs for businesses, with IDC estimating $75 billion will be lost in 2014 by U.S. enterprises dealing with data breaches. Meanwhile, another $22 billion is projected to be spent dealing with malware from counterfeit software. All told, businesses worldwide are expected to spend more than $491 billion because of malware associated with pirated software, $127 billion in dealing with security issues and $364 billion dealing with data breaches – with almost two-thirds of these losses being the result of criminal organizations.

Consumers and businesses have

33%

chance of encountering malware when they obtain and install a pirated software package or buy a PC with pirated software on it



24%

of network outages are caused by cybercriminals – leading to the highest per record costs from data breaches

[1] *http://riaa.com/physicalpiracy.php?content_selector=piracy_online_the_law*

Consumers will spend nearly

$25 billion

and waste

1.2 billion hours

in 2014 dealing with security issues created by malware on pirated software.

60%

of consumers put loss of data or personal information in the top three security fears

51%

placed unauthorized access or online fraud in the top three security fears

however...

43%

of consumers don't routinely install security updates on their computers

However, consumers are not immune from the staggering costs caused by cybercriminals. In fact, the same IDC report estimates consumers will spend $25 billion and waste 1.2 billion hours in 2014 dealing with security issues created by malware and pirated software. Symantec's Norton 2013 Cybercrime Report found that every year more than 378 million people are victims of cybercrime. And with IDC reporting 60 percent of consumers fear the loss of data or personal information from a security event, awareness is needed to promote safe computing habits.

Targeting Cybercrime

So what is being done to address the critical issue of cybercrime? Addressing nefarious activities is more of a behind-the-scenes effort involving government, technology companies, business leaders and consumers.

Microsoft, seeing an opportunity to protect customers and vulnerable populations, created the Digital Crimes Unit (DCU). The DCU works with industry partners, law enforcement, academia and governments to combat malicious software crimes (malware and botnets), intellectual property crimes, piracy and counterfeit software and technology-facilitated online child exploitation. In November 2013, Microsoft created the Microsoft Cybercrime Center as a center of excellence to advance the global fight against cybercrime.

What Can **You Do?**

Despite the threats associated with cybercrime, businesses and consumers are not powerless. Anyone, despite their IT background or profession, can decrease their risk of being the victim of cybercrime – without breaking the bank!

In fact, it takes just *three simple actions: regular updates, monthly security scans and using trusted retailers.*

1 Frequently install security updates for all your software

First is the simplest, and perhaps most effective, way to protect yourself – frequent security updates for all your software. Recommended updates should be downloaded directly from the manufacturer or publisher, or through your operating systems built-in update tool, to protect yourself from spoof sites that masquerade as updates. The easiest way to do this is by setting your computer to automatically update when new security patches are released. With a staggering 43 percent of consumers failing to routinely install security updates on their computer, this simple change in behavior can have tremendous impacts on the overall security of digital environments.

2 Keep your anti-virus software active and up-to-date, running regular security scans

Secondly, keep your anti-virus software active and up-to-date, and run regular security scans. Protecting yourself from viruses and malware also means not opening suspect email, or attachments from unknown sources. And users should perform at least one full scan of their computer a month, while software with real-time monitoring will better protect your online activities. Some newer operating systems, such as Microsoft's Windows 8.1, includes virus and malware protection, protecting your computer and saving you the cost of third-party anti-virus software. Additionally, completely shutting your computer down at least once a week will ensure your virus definitions and software is up-to-date and running correctly.

3 Purchase all hardware, software and computer services from trusted, reputable sources

Lastly, purchase hardware, software and computer services from trusted, reputable sources. Most manufacturers have a way to verify if a business is an authorized vendor, and if they're not, walk away – no matter how good a deal it is. Utilizing cloud-based software built and operated within the secure network of the publisher, like Microsoft's Office 365 productivity suite, is another way to defend yourself. Nearly one-quarter of enterprises, and 60 percent of consumers, purchased PCs from suspect sources, contributing to the risks associated with pirated software.

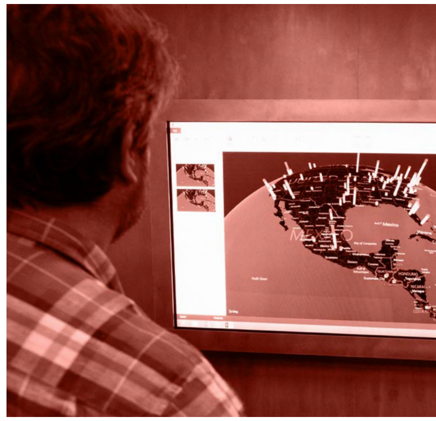
Bonus tip: *Business owners need to monitor what software their employees are bringing into the workplace, and into their network environment. Encourage employees to discuss any personal devices they plan to employ at work with IT.*

Additionally, businesses should monitor what software their employees are bringing into the network environment, and encourage employees to discuss any personal devices they plan to employ for work with their IT manager first. Developing a policy for computer security with guidance for employees on acceptable software downloads and activity will make all parties invested in the security of your digital environment. Small businesses without dedicated IT staff can also look into hiring consultants who provide assistance in software management and security practices. Businesses which regularly deal with sensitive customer data, including doctors' offices and retailers, can realize long term risk savings by incorporating this into their business planning expenses.

Ultimately, knowledge is power, and a few simple steps can have a tremendous impact on your information security. Technology is an area where if it sounds too good to be true, it likely is – and a little common sense goes a long way!

Learn more about cybercrime and how to protect yourself by checking out resources from your IT vendors and visiting Microsoft's www.microsoft.com/piracy.

If you suspect you've been the victim of cybercrime, you can report the fraud to the U.S. government's Internet Crime Complaint Center at www.ic3.gov.



In 2014, IDC estimates that enterprises will spend

$491 billion

because of malware associated with pirated software

which breaks out to

$127 billion

billion in dealing with security issue

and

$364 billion

billion dealing with data breaches

$315 billion

in enterprise losses will be the result of the activity of criminal organizations