The New Mafia: Gangs and Vigilantes

A Guide to Cybercrime for CEOs

Provided By

Malwarebytes TRAJECTORY

Table of Contents

Executive Summary

As the name implies, cybercrime is a technologically advanced iteration of traditional crime taking place in the virtual world. Though the nuances of cybercrime are unclear to many, the structure, execution and malice are reminiscent of those historically practiced within criminal organizations.

'The new mafia: gangs and vigilantes. A guide to cybercrime for CEOs' examines the rise of this activity and its ramifications for businesses and consumers. Through expert insight, this guide determines that the approach to stop cybercrime must reflect the path once taken to handle notorious gangs: fight back.

The Rise of Cybercrime

» Cybercrime has emerged from a nascent threat to an endemic global phenomenon, inflicting vast damage to businesses and individuals.

» The pace and pervasiveness at which cybercrime has emerged is creating a collective sense of worry among many consumers. While possibly overestimating the risks, more consumers find themselves scared, confused and intimidated.

» Attacks on businesses are growing. The number of attacks recorded in the first 10 months of 2017 has surpassed the total for all of 2016. The average monthly volume of attacks is up 23%. Businesses underestimate the extent to which they are targeted.

Emergence of the New Gangs

» Spawned from innocent beginnings, 'hacking' transformed into criminal activities through the 1980s and 1990s. In the early 2000s, the impact of expansive global attacks piqued the interest of criminals and nations alike.

» Four distinct groups of cybercriminals have emerged, serving as the new syndicates of cybercrime: traditional gangs, state-sponsored attackers, ideological hackers and hackers-for-hire.

Fighting back: Consumers and Businesses as the New Vigilantes

» To fight against cybercrime, both consumers and business must call upon their collective experiences, knowledge and awareness to supplement the actions of law enforcement agencies.

» Among consumers, awareness of cybercrime needs to shift towards a more honest and empathic perception of the risks and threats. Individuals need to feel encouraged to share and act, rather than be silenced by fear.

» Businesses must also heighten their awareness of cybercrime, taking a realistic view towards the likelihood of attack. The vast impacts of these attacks mean that cybercrime must be elevated from a tech issue to a business-critical consideration.

Introduction

With stories about daring hacks, pervasive breaches and massive data thefts increasingly dominating the headlines, cybercrime is fast stealing the curiosity and, unfortunately, the confidence of people everywhere.

The sophistication behind these criminal activities is beyond what most could previously envision. The power and global scale of cybercrime has enticed new entrants: criminal enterprises, nation states, ideological activists.

These organizations are relying on age-old tactics to achieve their aims: fear, confusion, intimidation and a collective feeling of helplessness. Legislators and law enforcement agencies are ramping up their fight against cybercrime, but perpetrators find ways to remain one step ahead.

However, businesses and consumers have more power in this fight than they realize. Their collective experiences, knowledge and awareness can help shed light into this activity and disarm cybercriminals.

By enhancing their understanding of the risks, the likelihood and true level of diligence required, individuals can feel more empowered to share insight that can increase protection. By acknowledging the devastating impact a cyberattack can have on the whole of an organization, businesses can devote the appropriate resources towards cybersecurity.

Throughout history, bands of determined individuals worked with law enforcement to bring down fearsome criminal enterprises. Today, businesses and individuals have the ability to be vigilantes of sorts against cybercrime. The success of global efforts to control cybercrime will depend on our ability to create an environment of openness that promotes the understanding, discussion and reporting of cybercrime.

This guide was constructed with insight from a global panel of Malwarebytes experts and external experts from a variety of disciplines. It also features a brief review of cybercrime history, the emergence of new participants and the impact on businesses and individuals.

The Rise of Cybercrime

From Emerging Threat to Global Phenomenon

What was once the reserve of hobbyists and enterprising individuals has taken a more sinister turn as the world has become more interconnected.

In the last decade, cybercrime has evolved from computer viruses that commandeered a select number of PCs to spectacular security breaches and cyberattacks that exceed the imagination.

What is disconcerting is the variety of participants that now engage in cybercrime. Captivated by the potential for financial gain, unprecedented control and the ability to cause widespread panic, criminal organizations, nation states and ideologists have made cyberspace their new preferred medium for nefarious activity.

As cybercrime becomes more sophisticated, more individuals and businesses are vulnerable. They are subject to attacks that are increasingly reliant on intimidation, powerlessness and fear, adopting tactics that criminal gangs once used to control entire neighborhoods and cities.

The rapid pace at which cybercrime has evolved is having harmful effects on the behaviors of both individuals and businesses. For individuals, the spread of cybercrimes has created a sense of fear that may overstate the risks. For businesses, the difficulty in identifying more sophisticated means of cybercrime may create a false sense of confidence.

Consumers: Reacting to the Perception of risk

Cybercrime impacts more of the businesses and services that consumers use on a daily basis. Yet, many individuals would not consider themselves to have experienced cybercrime. As Karuppannan Jaishankar, Editor in Chief of the International Journal of Cyber Criminology, puts it:

> *"Cybercrime is seen more as a fantasy, as many think it pertains only to machines and only hacking… most movies show more on the attack on the machines and less on humans."*

Indeed, cybercrime awareness is strongly influenced by the media. This idea goes as far back as the 1983 film WarGames, which historians believe played a significant role of shaping hackers in the mainstream for the next two decades. As we will see later, the concept of the 'hacker' came from more innocent beginnings. It was in the 1980s that mainstream news organizations began creating a negative connotation of the 'hacker', using the term to classify the typically young perpetrators of computer-driven crime. As author Steven Levy said, the media's usage of the term 'hacker' ensured that "the word quickly became synonymous with 'digital trespasser'."

Because first-hand experience with cybercrime is relatively low, factual coverage and fictional depictions end up playing a central role in shaping perceptions. According to David Wall, a professor of criminology at Leeds University in the UK, the perceptions created through popular media may lead to a misguided understanding of cybercrime:

> *"The science fiction molded conceptualization of cybercrime has shaped and distorted our expectations of them as being dramatic, futuristic and potentially dystopic… News reporting tends to simultaneously feed and feed off the public's lust for 'shocking' information… By blurring predictions about 'what could happen' with 'what is actually happening' the impression is given by news reports that novel events are far more prevalent than they really are."*

Most people are introduced or exposed to the idea of cybercrime via the news. According to a 2015 survey from Eurostat, just 15% of individuals surveyed had "not heard anything about cybercrime" in the news, compared to 85% who had heard about it through at least one of a variety of news sources, primarily television.

The issue with relying on the news for cybercrime awareness is that there is a tendency to emphasize sensational headlines, which often come at the expense of valuable contextual details. With the WannaCry attack of May 2017, for example, many outlets reported on the 200,000 infected machines in 150 countries, but fewer noted that hardly any money had been extracted – just £108,000 by August 2017.

The pervasiveness of these attacks and the increasingly interconnected nature of technology make consumers feel more at risk. As computer science academics Marcus Riek, Rainer Bohme and Tyler Moore noted, cybercrimes "are likely to be perceived as local crimes, because the internet is an open, global infrastructure in which all users can be affected."

In this heightened state of concern, skills and confidence dictate whether a consumer is more or less likely to be frozen by the fear of cybercrime. Those individuals that are less confident in their online abilities are quite likely to be concerned about becoming the victims of cybercrime. They are also less likely to engage in online commerce and other activity that may seem risky

In contrast, internet-savvy users are much more likely to recognize when they have been targeted by cybercrime and are more confident in reporting such instances.

Businesses: Misperceiving Vulnerabilities

The various ways that cybercrime can target businesses are theft of funds, data breaches, IP theft, and delays in identifying such attacks lead to some confusion around the size and scope of threats.

The growing sophistication of cybercrime and the ability of actors to evade detection mean that business often only discover that they are a victim months or years down the line. As Kris McConkey, global lead for threat intelligence and incident response at PwC states:

> *"In a lot of cases [of IP theft] the affected organization might not even know that they've had an issue, because all they've lost effectively is a copy of their design documentation and engineering plans and things. Actually, the real impact is then felt two, three, four, five years later when their competitor comes to market with something that's designed on top of their research investment, which could be billions of dollars.*

According to PwC's global economic crime survey, economic crime is falling; however, cybercrime is on the rise. 32% of the 6,000 respondents reported having experienced cybercrime in 2016, compared to 24% in 2014.

Data from Malwarebytes confirms the ongoing increase in cybercrime attacks on businesses. In the first 10 months of 2017, the number of attacks had already surpassed the total for all of 2016. The average number of monthly attacks has also increased by 23% in 2017. 2016 itself saw a spectacular rise in business-targeted cybercrime, with a 96% increase in attacks compared to the previous year.

The issue may be more widespread than businesses realize. Cybercrime figures vary across surveys targeting different areas of the business. For example, 74% of those surveyed in the PwC report which included various business stakeholders, reported that they either had not been or did not know whether they were victims of cybercrime. In contrast, Malwarebytes research, using a sample of CIOs, IT managers & directors, and CISOs, found that the proportion of businesses who state they have experienced no cybercrime is much smaller, between 21% and 35%, across the four nations covered by the survey.

These variances point towards potentially dangerous gaps in understanding the threat of cybercrimes across an institution. This lack of knowledge may lead to a potential underreporting in cybercrime. The problem may be much more widespread than most business leaders realize.

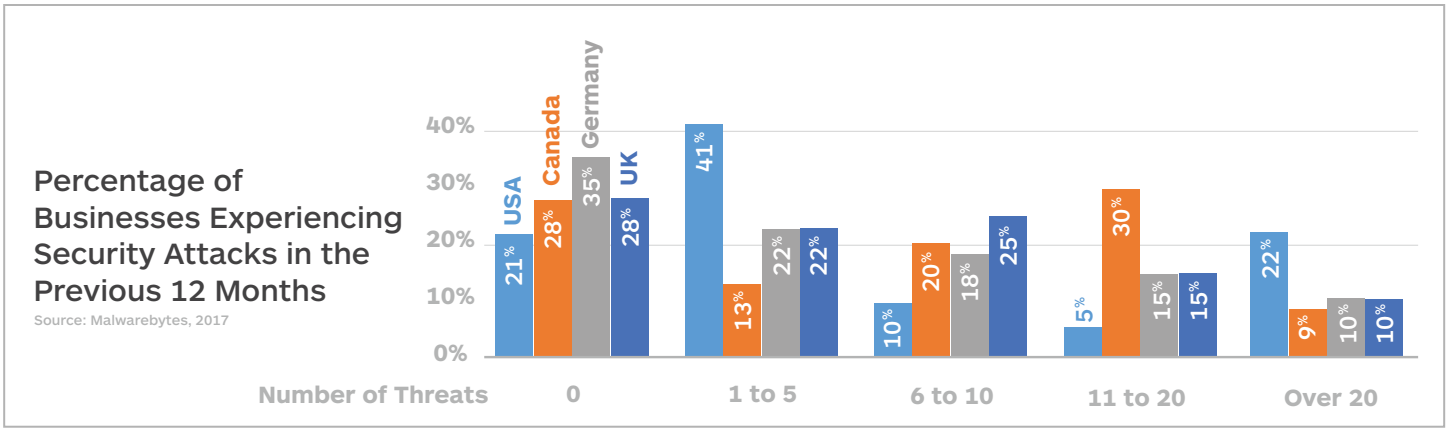


Figure 1: Security Attacks That Have Occurred During Previous 12 Months

Emergence of the New Gangs

The entrance of new participants has transformed cybercrime from isolated and individualized acts into pervasive, savage practices run by distinct groups of individuals.

Similar to the criminal gangs that dominated major cities like New York in the 1930s, these new participants have largely been attracted by the potential for riches and power. Likewise, these newer perpetrators of cybercrime have increasingly resorted to fear, intimidation and a feeling of helplessness to achieve their aims. Similar to the mobsters who would muscle their way into a business and make demands, cybercriminals are taking command of computers and sensitive personal information to threaten victims.

These distinct groups, traditional gangs, state-sponsored attackers, ideological hackers and hackers-for-hire, have become the new gangs of cybercrime. While defined by unique sets of motivations, each syndicate employs a vast, constantly evolving array of tactics to infiltrate, strongarm and create terror.

A Brief History of Cybercrime

While the headlines associated with computer hacking, the universal tool of cybercrime, are almost universally in relation to criminal activities, its roots are significantly more innocent.

The concept of hacking began at the Tech Model Railway Club at the Massachusetts Institute of Technology (MIT) in the late-1950s. Far from being an anonymous figure behind a screen, a 'hacker' was someone who worked on the signals and power element of the model railroad, finding technological solutions to manipulate and improve the model.

Around the mid-1970s, experts were starting to realize the manipulative potential of computers to orchestrate significant financial crimes. Stanford researcher, Donn B. Parker's 1976 text, Crime by Computer: Startling new kinds of million-dollar fraud, theft, larceny & embezzlement, identified serious security issues heralded by mainstream computer use. At that point, the book had already identified more than 1,000 cases of computer crime around the world.

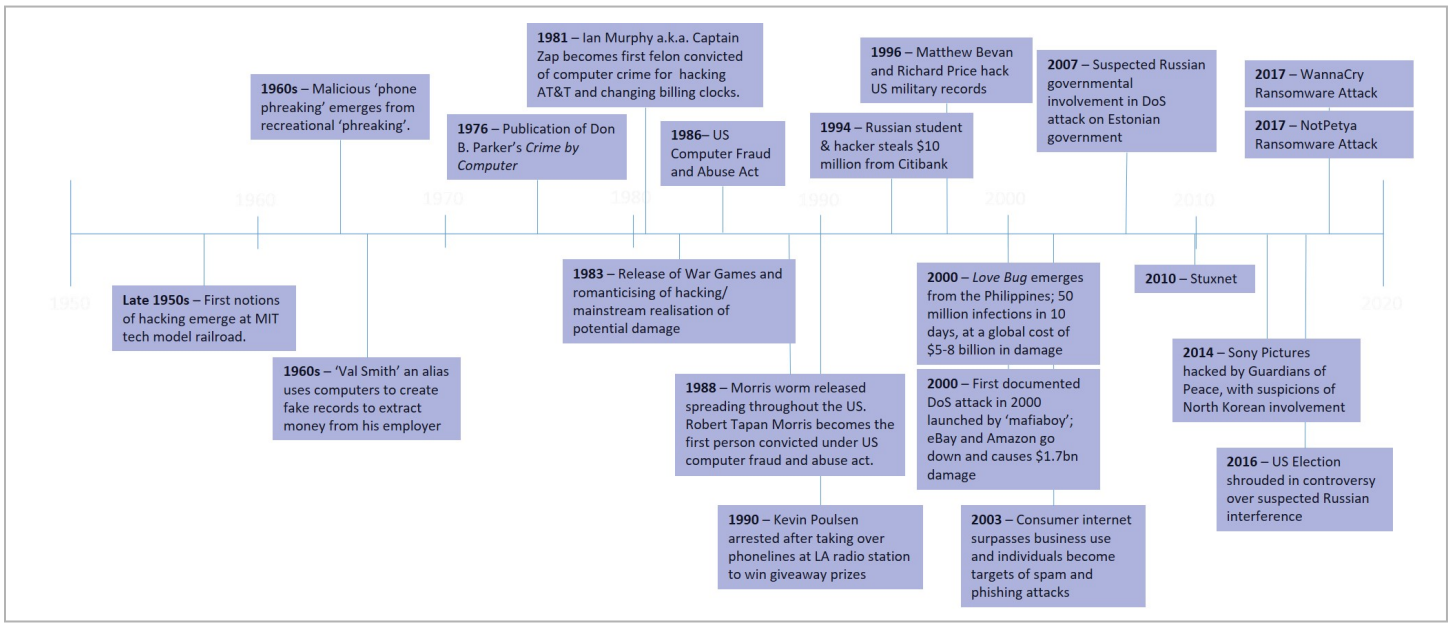
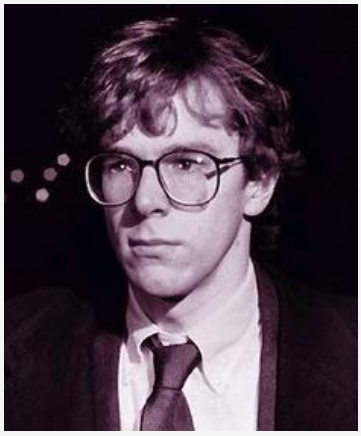


Figure 2: Cybercrime Timeline

Case Study: The Morris Worm

Released in the USA in 1988, the Morris Worm was one of the first computer worms distributed via the internet, and the first to gain significant mainstream media attention. According to Robert Morris, the worm was not created to cause damage, but to gauge the size of the internet – though he still attempted to disguise his authorship. The worm wreaked havoc on the young internet, infecting 2,000 computers in 15 hours, there were only around 60,000 computers online, causing anywhere between $100,000 and $10,000,000 of damage. Morris was charged under the Computer Fraud and Abuse Act, and sentenced to three years' probation, 400 hours of community service, and fined $10,050 plus the cost of his supervision.



The 1980s were a watershed decade for computer crime, as a new breed of 'hackers' emerged. These individuals were more focused on personal gain through the pirating of software, the creation of viruses, and the theft of personal information. These illicit activities ramped up in the 1990s, with online financial crimes growing significantly – most notably with the theft of over $10 million from Citibank by Russian student Vladimir Levin.

As consumer use of the Internet surpassed business use in the early- and mid-2000s, the occurrence of spam emails accelerated. In 2002, 29% of all emails were spam; by 2008-10, this figure was 90%. Increased awareness has sent this figure plummeting in recent years.

Yet, hackers and cybercriminals had already moved on to more sophisticated, and well organized, modes of attack. Significant markers included the development of botnets that were crucial to the orchestration of two of the biggest cybercrime events in the 2000s; the ILoveYou bug and the very first Distributed Denial of Service (DDoS) attack allowed spammers to commandeer large numbers of computers and carry out repetitive, volume-based, rather than targeted scams, in order to maximize revenues.

It is at this stage that the emergence of these new syndicates began. Tim Jordan, Professor of Digital Cultures at the University of Sussex in the UK, describes how online gambling led to a growth in interest in cybercrime among organized crime groups and, to an extent, nation states.

"Early on, the literature on cybercrime was mainly about how the fear was far greater than the actuality through the 1990s to the mid-2000s. But there was a period when online gambling started to become a serious concern and that seems to have brought organized crime into contact with various hacking groups. Sections of the hacking community for whom crime had really been limited to what they needed to do to get access to information became very associated with organized crime as organized crime realized there was a lot of money to be made. What then seems to have happened is that in the same way that various hacking groups got involved with organized crime, a number of similar people have become involved with the nation-state, particularly in Russia."

Case Study: ILoveYou

Released on the 5th of May 2000, ILoveYou, also known as the Love Bug or Love Letter, emerged from the Philippines, attacking tens of millions of Windows computers via an e-mail message with an attachment which overwrote random types of files, before sending a copy of itself to all of the addresses in Windows Address Book, causing it to spread rapidly. The worm was thought to have caused $5.5 – 8.7 billion in damages worldwide, with a further $15 billion required to remove the worm. The perpetrators, two Filipino computer programmers named Onel de Guzman (right, above) and Reonel Ramones (right, below) were arrested almost immediately. However as there were no laws against writing malware in the Philippines at the time, all charges were dropped. Just two months after the attack, the Philippine Congress enacted Republic Act No. 8792, known as the E-commerce Law, and in 2002, the virus obtained a world record as the most virulent computer virus of all time.

Since the entry of these new participants, security breaches and cyberattacks have grown in scale, complexity and malice. Ransomware is emerging as the latest tool of choice for cybercriminals. The rate of ransomware attacks, as detected by Malwarebytes, exploded by 289% in 2016. In fact, between September 2015 and September 2017, the number of ransomware attacks detected had increased by 1,988.6%. And as of 1 November, the number for 2017 has already surpassed the total for 2016 by 62%.

Ransomware has largely replaced the use of botnets, which decreased by nearly 50% in 2017, as of 31 October.

These figures, as well as the high-profile WannaCry and Petya attacks of 2017, illustrate just how quickly the methods of cybercrime can evolve and how rapidly problematic they can become for people around the world.

Ransomware Threat Count

Source: Malwarebytes 2017

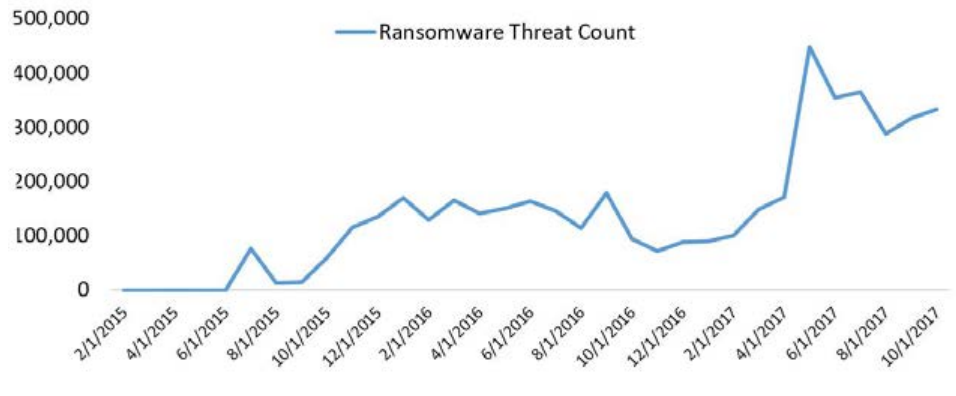


Figure 3: Ransomware Threat Count

The Four Gangs

> *"In the old days, people robbed stagecoaches and knocked off armored trucks. Now they're knocking off servers."*
>
> – Richard Power, Computer Security Expert and Author

In many cases, the new gangs are shifting classic criminal activities, theft, money laundering, ransom, into a new medium. These groups of cybercriminals have also developed entirely new methods of attack, such as computer viruses, worms, or DDoS attacks.

These new syndicates are characterized by: the presence of an organizational structure akin to crime families, the sophistication of hacking, the emergence of a highly professional service economy for cybercrime, and the co-option of these services by ideological groups and nation-states.

Collectively, these gangs form an incredible diverse, incredibly dangerous set of online operators, with motivations as different as their backgrounds.

Traditional Gangs

These groups have taken the motivations and acts of traditional organized crime gangs, theft and the sale of drugs, guns and stolen goods, to the online world. Often coming from organized crime backgrounds, they operate in a structure and manner similar to their street predecessors.

Criminals follow the money, cybercrime is no exception. A 2014 paper written by the National Security Research Division at the Rand Corporation states that the online black market was:

> *"Once a varied landscape of discrete, ad hoc networks of individuals motivated by ego and notoriety, has now become a burgeoning powerhouse of highly organized groups, often connected with traditional crime groups (e.g., drug cartels, mafias, terrorist cells) and nation-states."*

These gangs are composed of groups of hackers that have sought to monetize their abilities together and pre-existing crime groups that have been able to co-opt those with the necessary skills in order to maintain their position despite the disruption brought by the internet. The people at the top may be the same individuals leading drug cartels or pre-existing gangs, or new kingpins that have risen to the top of organizations as the internet has grown.

In any case, it is those at the head of these organizations who officially keep their hands clean, while many, perhaps the same individuals involved in traditional, recreational hacking, are those likely to be carrying out attacks and facing the consequences if caught.

State-Sponsored Attackers

The last three years have seen a massive rise in attacks by state-sponsored attackers with the aim of stealing information and disrupting political activity. Russian interference in the US Election and widespread hacks from North Korea are prominent examples.

The activity of state-sponsored attackers tends to be more subtle than other gangs – yet, as Kris McConkey, Global Lead for Threat Intelligence and Incident Response at PwC notes, this activity can have a similarly detrimental impact.

> *An example of this could be a foreign government seeking to support its local aviation industry, to disrupt aeroplane manufacturers' stranglehold on the narrow body aircraft market. Such a government might be very interested in stealing a lot of plans and blueprints detailing how the leading narrow body aircraft actually work, so it can feed that information to its local competitors; the aim being to bring a competing aircraft to the local market first, and then the international market.*

Beyond the international espionage that typically comes to mind with state-sponsored activity, these hackers are increasingly interested in corporate theft and sabotage. The consequences of such attacks such are only felt months or years later as competitors take advantage of important research and development, or strategic information. Businesses must be more aware of these syndicates than they might realize.

Nation-state cybercrime is a prominent issue, and it is not limited to governments of questionable repute. For example, the Stuxnet computer worm designed was deployed by Western nations to cause Iran's nuclear centrifuges to spin too quickly, destroying the centrifuges, and infecting 200,000 computers.

This act revealed the vulnerability of physical infrastructure to cybercriminal activity and according to Guido Gluschke, the Director of the Institute for Security & Safety at Brandenburg University of Applied Sciences, such targets could suggest a potential blurring of the distinction between cybercrime and cyberwarfare:

> *"Hospitals can be seen as critical infrastructure and ransomware is more associated with organised crime or cybercrime activity, so at this point the line between cybercrime and cyberwar begins to blur."*

Ideological Hackers

These gangs are renowned for gathering and leaking classified information on governments and high-profile organizations that can ultimately destroy reputations. These groups act on the basis on moral and ethical duty. Often, they attempt to use the threat of classified leaks to coerce governments and individuals to act in their favor.

Avoiding the crosshairs of these groups can be particularly difficult, given the wide spectrum of moral and political beliefs that exist in the world today. Wikileaks was started as an effort to fight corruption through 'principled leaking.' For many citizens, this seems noble; yet for a business with sensitive trade secrets or involvement in national security, the release of classified information by unelected hacking groups may be less than ideal.

In a time of enormous political polarization, it will be increasingly difficult for governments and businesses to steer clear of ideological cybercrime. In this context, groups at political extremes are more likely to firstly, disagree ideologically with political and business developments and secondly, attack the online presences of those they disagree with.

The variety of groups in this category of gangs will only expand. Protest movements, right-wing, left-wing, liberal, conservative, anti-capitalist, animal-rights etc. will increasingly take their real-world activism online, with online manifestations of real-world protest, such as obstruction and reputational damage likely to come in the form of online attack.

Hackers-for-Hire

One of the biggest developments in cybercrime is the growth of a highly-professionalized service economy for cybercrime services. The proliferation of the 'dark web' has spawned a market for activities such as hacking, malware, and the use of botnets for spam and DDoS attacks.

These individuals are akin to paid guns for hire. Interestingly, they operate in a highly retail-oriented manner with an emphasis on customer service and reliability. Many vendors offer money back guarantees if a service does not perform to the expected standard or if an antivirus engine detects the malware within a certain period of time.

The most important aspect of this development is the removal of technical knowledge as a barrier to cyber criminality. Budding criminals no longer have to learn the appropriate skills, instead they can outsource the technical execution of their schemes to hackers-for-hire. Nation-states have increasingly become more active in tapping into these services.

The advent of 'Ransomware-as-a-service' is proving to be a vastly active and lucrative area for these hackers. Figures from Malwarebytes show that the average number of ransomware attacks detected monthly increased by 94% through October 2017, compared to 2016 data.

The extent to which businesses, nation-states and others are hiring or co-opting these groups for sophisticated cyberattacks is unclear, making it difficult to understand the size and impact of this market.

Fighting Back: Consumers and Businesses as the New Vigilantes

The Power of Collective Intelligence

Historically, many gangs met their fall at the hands of select law enforcement individuals. From Eliot Ness and the Untouchables taking on Al Capone to the Italian prosecutors that boldly went after the Sicilian Mafia in the early 90s, these groups were vigilantes of sorts, willing to go above and beyond to fulfill their mission of justice.

Countless individuals played an important role, providing these lawful vigilantes with information and guidance that ultimately proved useful in tracking down elusive figures.

While most law enforcement agencies and regulatory bodies have developed specialist teams devoted to cybercrime, the highly fragmented, global nature of technology makes it much more difficult to identify and thwart these illicit activities.

This is where the power of the people comes into play. Individuals and businesses alike can help the global effort against cybercrime groups by sharing their collective experiences to build knowledge and awareness. Creating an environment where the risks are better communicated and understood will enable individuals and businesses alike to better identify and ward off threats.

Individuals and businesses have first-hand knowledge of cybercrime that can prove invaluable to the creation and sharing of intelligence. Law enforcement agencies will continue to make great strides, yet individuals and businesses have the power to change mindsets and help take protection into their own hands.

Consumers: Getting Honest and Vulnerable about Cybercrime

Because cybercrime is relatively emergent compared to more traditional forms of crime, there is still some reticence among legislators to acknowledge the true emotional and financial toll. As such, cybercrime is often more challenging to prosecute and victims may feel much more powerless.

Debarati Halder, the Managing Director of the Centre for Cyber Victim Counselling in India, notes the differences in how both victims and legislators perceive cybercrime:

> *"There is less awareness about the legal status of these [cyber]crimes, some of which like bullying or revenge porn are not even addressed properly by the law of many jurisdictions. This understanding differs from real-life crime in my opinion. In real-life people actually feel the physical pain and, in certain cases, emotional injury when harassed face to face… Evidence can be seen and collected by the police, and perpetrators can be more easily identified by the victims, with these crimes more easily proven in court than cybercrimes."*

This potentially vague understanding of cybercrime has a significant impact on the way in which the public treats victims, and how victims consider themselves. A Malwarebytes researcher explains how shaming can be unproductive in the fight to protect ourselves and prevent cybercrime:

> *"Public shaming of the victims is a mistake. It may be that they have done nothing wrong. No one is immune. It is much better if it is treated as a learning experience and people share what has happened to them. That's how we will stop the criminals, by knowing as much as possible about the attack, as soon as possible."*

As we noted earlier in the report, those Internet users who are more confident in their online prowess are much more likely to identify and even preempt attacks. Thus, an environment where confidence is created rather than subjugated will ultimately help build esteem, awareness and preparedness towards more types of cybercrime.

An honest and empathic perception of cybercrime can help stoke the flow of information. By recognizing their own technological vulnerabilities, individuals can acknowledge that perhaps a victim wasn't a victim because of foolishness or a lack of working knowledge. By sharing their experiences without fear of reprisal, victims can help create narratives that help individuals understand the real-life costs of cybercrime.

Likewise, those people that are threatened by ransomware and other modes of attack should feel encouraged to report their attacks, rather than just pay for their silence. This information can prove invaluable to others in recognizing potential attacks and informing the efforts of law enforcement officials.

Groups will always work to be one step ahead of legislators, law enforcement officials and others. Yet, the sharing of experience leads to knowledge and confidence that greatly enhances the ability of individuals to protect themselves. Dialogue is their way to take up arms in the fight against cybercrime.

Businesses: Recognizing that Cybercrime is a Business, not a Technological Issue

The variety of attacks, the vast length of time they can strike at a business and the numerous costs should force business leaders to consider some hard truths about cybercrime.

As noted earlier in the report, there is a wide contrast between the number of business leaders and the number of technologists that recognize and/or acknowledge cybercrimes. The tendency for technologists to be much more honest about the potential for cybercrime reflects an idea shared by many of the experts interviewed for this report: cybercrime is considered the domain of CIOs and IT departments.

This is a flawed approach. The extent of cybercrime and the depth of the strategies needed to combat must be central to general business strategy – thus, it must become the domain of chief executives. Nir Kshetri, a Professor of Economics at the University of North Carolina, confirms this view:

> *"In business too many people think of cybercrime as a 'technical' thing. Something for the CIO, but not the CEO. It needs to become a mainstream management issue."*

This point is further evidenced by data produced by Malwarebytes which highlights the severity of impacts of cybercrime. Major impacts such as reputational damage, financial loss and legal costs are cross-business implications that should be managed by CEOs.

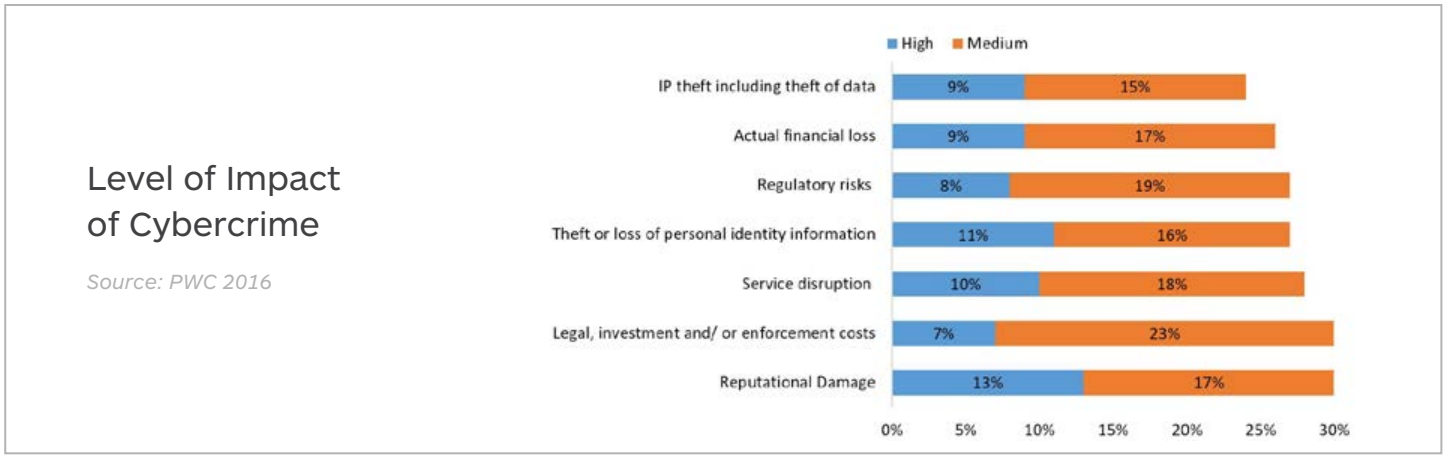


Figure 4: Level of Impact of Cybercrime

Knowledge of cybercrime and security best practices has to go across the organization, driven from the top down. With an endless array of potential vulnerability points, from reception to external vendors, an exchange of knowledge, awareness and insight is key to recognizing threats.

This idea of a CEO as a cybersecurity champion evokes an even bigger shift which can ultimately help businesses better protect themselves: treating cybersecurity as an investment in trust, rather than a way to prevent losses or costs. Thinking otherwise is a mistake, according to one Malwarebytes researcher:

> *"IT is regarded as a cost center in most businesses. That is a mistake. IT is an investment in public trust on which capital is built."*

Cybercrime erodes consumer trust. Strong protection enhances it. Treating cybersecurity as a business investment rather than an IT consideration helps reimagine such deployments in a way that not only enhances protection, but encourages customer confidence and interaction.

Instead of closing gaps and filling holes, businesses have the opportunity to go on the offensive in the battle against these groups. A greater understanding among business executives about the true potential and recognition of cybercrime can help encourage and build awareness across multiple industries.

Looking Ahead

Technology will only become more prevalent in our lives, as innovations such as the Internet of Things, machine learning and automation arrive. Undoubtedly, these mediums will spawn the next generation of cyberattacks from the new gangs. However, individuals and businesses are far from helpless.

This next generation of attacks stands to be more invasive and more personal. For example, connected devices implanted within human bodies, such as artificial limbs or aortal valves, may possess the same vulnerabilities to control and manipulation as the Iranian nuclear reactors did to Stuxnet. It's not far-fetched to believe that someday, a syndicate can take control of a vital health device and hold an individual ransom.

The idea is frightening, but once again, this is where individuals can take more control. The confidence of consumers and businesses to identify and report cybercrime helps reduce the proliferation of cyberattacks.

To succeed, mindsets must change. As noted earlier, there is a difference in the way in which society understands these cyber threats in relation to traditional forms of crime. Individuals that once felt inclined to internalize the shame must be encouraged to share information and take action.

Businesses who aren't able to immediately identify the impact of cybercrime must still believe that the threat is real and invest accordingly.

Without accepting, sharing and learning from our experiences, these groups will continue operating in the shadows. Dialogue is needed to normalize and demystify these activities in order to better understand new threats with new perpetrators and new motivations.

Knowledge, awareness and intelligence are our best weapons against the new gangs of cybercrime. Given the fragmented, global nature of cybercrime, individuals and businesses have to play an important role alongside law enforcement agencies governments and other bodies in thwarting this activity.

Rather than sit back and minimize the blow from cybercrime, individuals and businesses must take the same actions that previous generations of vigilantes once did against the fearsome syndicates of their day: fight back.

Photo Acknowledgements:
Robert Tappan Morris; UK Fast, 5/23/2012
Onel de Guzman: BBC News, 5/10/2000
Reonel Ramones: AP Archive, 5/9/2000