The evolving landscape of technology-dependent crime

How to cite :- Steven Furnell. 07 Dec 2016, The evolving landscape of technology-dependent crime from: The Routledge Handbook of Technology, Crime and Justice Routledge

Accessed on: 18 Dec 2018
https://www.routledgehandbooks.com/doi/10.4324/9781315743981-4
The evolving landscape of technology-dependent crime

Steven Furnell

This chapter examines the evolving relationship between information technology and its technology-specific modes of harm and criminality. These so-called ‘cyber-dependent’ offences can involve a broad spectrum of activities, everything from the creation and distribution of malware, to distributed attacks and the targeted disruption of networks. The discussion examines the current situation (and aspects of the path that has led us towards it), with particular reference to the technologically driven and technologically based nature of the offences involved.

Technological growth: a foundation for future attack

When we look at technology-dependent threats, one of the first things to realise is that there is a great deal of technology out there to be targeted and potentially exploited. To illustrate the point, statistics from the International Telecommunications Union (ITU 2015) reveal the following trends in terms of ICT growth since the millennium:

- A seven-fold increase in global Internet penetration (i.e. individuals using it) from 2000 to 2015, up from 6.5 per cent to 43 per cent. In terms of the raw numbers, Internet users have increased from 400 million to 3.2 billion in the same period.
- Domestic Internet access increased from 18 per cent in 2005 to 46 per cent in 2015.
- 97 per cent penetration of cellular phones, up from 738 million in 2000, to over 7 billion in 2015.
- Mobile broadband subscriptions increased 12-fold since 2007, reaching 47 per cent penetration in 2015 (noting that, by comparison, fixed-line broadband had only reached 11 per cent penetration by the same point). In parallel, 69 per cent of the worldwide population were within coverage for 3G mobile data, compared to less than half just four years earlier.

In all of these cases, the figures are based on the worldwide averages, and there are of course notable variations in specific cases. As may be expected, the penetration within developed countries is substantially higher than developing or least developed countries, with over 80 per cent of the population online in the former, as against approximately a third and a tenth in the latter cases.
Steven Furnell

A consequence of these advances, especially when looking at the population in the developed world, is that we expect to be online, and we expect to use the related devices and services. Unfortunately, however, we are often not so prepared when it comes to an expectation to secure and protect them. Indeed, the increased usage has not necessarily been accompanied by a corresponding growth in the associated security, and so there is arguably a far greater population of users and devices that have the potential to fall victim to cybercrime and other forms of online attack.

Classifying the crimes

Part of the challenge of examining cyber-dependent crimes (and indeed other security breaches such as insider abuse and frauds) is that the domain itself gives rise to variations in the use of terminology. This in turn can lead to confusion over what should be counted, and the potential for resultant misrepresentation has existed for some time. Even taking a look at just the subset of threats relating to malware serves to reveal the challenge of the situation. For example, some terms (e.g. virus, worm and Trojan) are technical definitions, insofar as they group programs according to how the code functions. In this respect at least, there is common agreement across the industry. However, sometimes other, non-technical, terms are used to describe malware and malware-related programs. The term ‘spyware’ is one such example of this. As the name suggests, it refers to software that monitors activity on a computer. Unfortunately, this could include programs that are malicious and those that are not (such as monitoring agents that may be deployed on end-systems within an organisational network).

In 2001, the author’s book *Cybercrime: Vandalizing the Information Society* (Furnell 2001) aimed to provide an introduction to the cybercrime problem and to explore some of the main dimensions in which problems could be encountered. As such, there was coverage of core themes such as hacking and malware, along with various examples of (then) relatively new problems such as website defacement and Distributed Denial of Service (DDoS) attacks. However, looking at the book today, it really does seem a reflection of a more innocent age (although it did not seem like it at the time). The coverage predates a whole range of topics that one would now consider fundamental to the topic of cybercrime, and the wider threat landscape. As examples of just a few things that the book does not cover, one can list phishing, mobile malware, and Advanced Persistent Threats – three issues that it would be inconceivable to omit from a discussion of cybercrime in today’s context. However, one aspect of the book that appears to remain relevant is the way in which it presented a top-level stratification of the cybercrime problem, splitting it into those crimes that are assisted by the presence of computers, and those that have emerged as a direct result of them. This distinction is maintained in much of today’s discussion of the problem, with relatively recent definitions from the UK’s *Serious and Organised Crime Strategy* (HM Government 2013) maintaining similar descriptions but with more up-to-date labels. The related definitions are presented and contrasted in Table 3.1.

Viewed within this terminology, this chapter is focusing upon the subset of cyber-dependent (computer-focused) crimes. However, while the discussion will continue to use the terms, it is worth briefly considering the validity of this distinction, because the distinction is arguably less meaningful now, given that the wider crime can involve many methods. For example, in the case of a banking Trojan, do we view the malware as the crime, or what it does, or both? With malware being created and distributed to serve underlying criminal motives of computer-enabled fraud and theft, the boundary can blur quite easily. Another contributor to this blurring is that some of the channels for cyber-dependent crimes can also support cyber-enabled crime as well, for example, both malware (cyber-dependent) and phishing (cyber-enabled) can be
encountered by email. Thus, from the victim perspective, the distinction between them is arguably less meaningful in practice; they can both be seen as email-based threats. As such, while the naming potentially fits for the purposes of developing a taxonomy, it is relevant to consider how much utility it actually has in practice (e.g. is it aligned with how individuals and businesses think of cybercrime?).

Framing things in terms of cyber-dependent and cyber-enabled is focusing upon the means of attack, rather than the motivation and intended outcome — and it is arguably the latter aspects that will interest people in terms of understanding why they might fall victim and the consequent case for protection. Moreover, if we look at a particular attack in more detail, we can often find multiple means being employed in pursuit of a single outcome. For example, distribution of malware may be used to establish a botnet, which may in turn be used to launch DDoS attacks against nominated targets. While there are several affected parties here (e.g. anyone who receives the malware, and particularly those whose systems get infected and become part of the botnet), the main impact is arguably felt by those that find themselves on the receiving end of the resulting DDoS attack (for whom the resulting outcome could range from system outage and disruption, through to loss of revenue and reputational damage). It is also possible to imagine a scenario that intermixes cyber-dependent and cyber-enabled methods within the conduct of a single attack. For example, a phishing attack could be used to acquire a user’s login credentials, which in turn lead to a hacking incident, that results in data theft from the victim organisation (with the data itself potentially going on to be used in other ways, e.g. to commit fraud). Indeed, a key part of the evolution over the past few years has been the interplay between the categories. For example, Ransomware (as exemplified by cases such as CryptoLocker\(^1\)) introduces a clear overlap between a technically dependent form of attack and the rather more long-standing financial motive of extortion. The latter is certainly not a cyber-dependent crime, but doing it in this manner, underpinned by malware-style techniques for propagation and payload, certainly depends upon the technology to achieve it.

Ultimately, therefore, a cyber-dependent technique can result in the same impacts as a cyber-enabled one, or they can be used together to the same effect. This view was very much reflected within a 2015 study funded by the UK Home Office, which sought to examine the appropriate means of understanding the scale, trends and measurement of cyber-dependent crime (Furnell et al. 2015). As part of the investigation, views were canvassed from a variety of professionals and practitioners from the anti-malware and wider Internet security industry, and

---

**Table 3.1 Similarity across the years – top-level categorisations of cybercrime**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer-assisted crimes.</strong> Cases in which the computer is used in a supporting capacity, but the underlying crime or offence either predates the emergence of computers or could be committed without them.</td>
<td><strong>Cyber-enabled crimes</strong> are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT.</td>
</tr>
<tr>
<td><strong>Computer-focused crimes.</strong> Cases in which the category of crime has emerged as a direct result of computer technology and there is no direct parallel in other sectors.</td>
<td><strong>Cyber-dependent crimes</strong> are offences that can only be committed by using a computer, computer networks, or other form of ICT ... Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud.</td>
</tr>
</tbody>
</table>
Steven Furnell

one of the observations emerging was that the provided examples of cyber-dependent crime (e.g. malware, DDoS and hacking) were in fact crime *tools* rather than crime *types*. While this viewpoint clearly contradicts the definition from the *Serious and Organised Crime Strategy* (and indeed legislation that would classify these activities as criminal acts in their own right), it also serves to further highlight the significant perceptual differences that exist around the topic.

One of the factors contributing to the inconsistency of the terminology and vocabulary is the dynamic nature of the domain. The appearance of new threats leads to new names being introduced, and further potential for confusion arises from the industry itself seeking to differentiate its product and service offerings. This point is well-illustrated by the following quote from one of the respondents in the aforementioned Home Office study:

> Most vocabulary seems to come from Vendors’ Marketing teams … as new vendors think of better ways of dealing with security they need to change the view of security professionals to fit in with their paradigm.  
>
>(Furnell et al. 2015: 9)

Although this could be taken to be an implicit criticism of the vendors concerned, the reality is that both they and the victims of the attacks are sitting within an environment that will not stay still. In fact, new names are often *required* in order to enable a distinction to be made between new approaches and those that preceded them. As such, while a high-level classification of crimes as cyber-dependent and cyber-enabled can be valid as a conceptual distinction, it is often less meaningful in practical terms. If a distinction is to be made between *-dependent* and *-enabled* categories, then it is perhaps more meaningfully applied to the underlying methods, leaving the *crimes* to be considered as cyber-related, regardless of how they happen (recognising that as time goes on, more and more criminal activity is likely to have a cyber component involved in it).

**Whatever we call it, it’s getting worse**

Setting aside the specific debate around naming the cyber-crimes, one thing that is clear is that there can be lots of them. There is now a much greater diversity in how the problems are categorised. To illustrate the point, Table 3.2 lists the various categories used by three long-standing and widely cited survey series, all of which give attention to cyber-dependent crimes alongside other types of security incidents (with the table presenting only those categories with potential to relate to the former). While it is possible to identify some points of direct comparability between the lists (e.g. all three have a distinct category relating to malware), there is also a very clear variation in the nature and granularity of the groupings across the set. At the time of writing all of the categories would remain valid, but the picture of cybercrime that emerges would have the potential to look quite different depending upon the lens that is used. It is also worth noting that even here, some of the categories (e.g. ‘exploit of user’s social network profile’) could end up capturing both cyber-dependent and cyber-enabled crimes, depending upon what exactly was done in a given attack.

So, while we do not have a definitive list of cybercrime and attack types, we do nonetheless have a growing one. Even then, however, the snapshot of categorisations provided by Table 3.1 only gives part of the picture, and in order to get a feel for the evolution of the problem, it is worth looking at how the *level* of reporting against the different types has changed over time. As an example, we can look in more detail at the related numbers from the Information Security Breaches Survey (ISBS) series, which has been carried out amongst UK organisations since the early 1990s. Figure 3.1 tracks the related survey categories across the last decade, based
Table 3.2 Cyber-dependent crime categorisations from leading survey series

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Malware infection</td>
<td>• Cyber attacks to disrupt or deface the organisation</td>
<td>• Infection by viruses or malicious software</td>
</tr>
<tr>
<td>• Bots/zombies within the organisation</td>
<td>• Cyber attacks to steal financial information (credit card numbers, bank information, etc.)</td>
<td>• Actual penetration into the organisation’s network</td>
</tr>
<tr>
<td>• Password sniffing</td>
<td>• Cyber attacks to steal intellectual property or data</td>
<td>• Denial of Service attack</td>
</tr>
<tr>
<td>• Denial of Service</td>
<td>• Internal attacks (e.g. by disgruntled employees)</td>
<td>• Attack on Internet or telecommunications traffic</td>
</tr>
<tr>
<td>• Website defacement</td>
<td>• Malware (e.g. viruses, worms and Trojan horses)</td>
<td></td>
</tr>
<tr>
<td>• Other exploit of public-facing website</td>
<td>• Zero-day attacks</td>
<td></td>
</tr>
<tr>
<td>• Exploit of wireless network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Exploit of DNS server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Exploit of client web browser</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Exploit of user’s social network profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Instant messaging abuse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Insider abuse of Internet access or email (i.e. pornography, pirated software, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Unauthorised access or privilege escalation by insider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• System penetration by outsider</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes: (a) Richardson (2010); (b) Ernst & Young (2014); (c) HM Government 2015

Figure 3.1 Tracking the cyber-dependent crime categories from the Information Security Breaches Survey series

- Infection by viruses or malicious software
- Actual penetration into the organisation’s network
- Denial of Service attack
- Attack on Internet or telecommunications traffic
upon the reported data from large organisations (those with 250+ employees). The surveys all included responses from small and medium organisations as well, but differed in whether they reported these distinctly, or included them within an overall figure (whereas the data for large organisations was consistently separated across all editions of the report). The chart focuses upon categories that were consistently reported across the surveys (another ostensibly cyber-dependent category, ‘significant attempt to break into the organisation’s network’, also appeared in the surveys from 2006 through to 2013, but was dropped in the later versions).

It should be noted that the frequency of the survey changes partway through the period, because it began as a biennial publication and then became an annual study from 2012/13 onwards.

As indicated earlier, we cannot be definitively sure that all of the incidents are exclusively related to cyber-dependent crimes. For example, some of the reports relating to the penetration of the organisation’s network could have resulted from staff disclosing login credentials in response to phishing messages, and the penetration could in turn have led to data theft (so the predominance of the activity would be cyber-enabled, with the penetration just being the means to an end).

When looking at these figures in the context of the wider ISBS findings, it should be noted that they are not necessarily the most prominent categories of attack, nor necessarily the ones considered to be the worst or most costly to the organisations concerned. However, when assessing the evolution of cyber-dependent crime, the key thing to note is basically the trend over time – and the fact that nothing appears to have got better when considered on balance across the decade, and reported incidence in all of the categories has ended the period at a significantly higher level than it began. This occurs in spite of organisations reporting increased use of controls, and serves to evidence the challenge of keeping up with the problems. This will also have been further complicated by the broadening of the technology landscape to be protected, with the increased use of mobile devices, the emergence of cloud computing, and increased IT outsourcing, all being trends that were observed across the period and adding to the complexity of safeguarding IT security. Basically, the advancements can open up new opportunities for attack and exploitation, bringing advantages for the cybercriminals, while those seeking to ensure protection have to fight harder to keep pace with change.

A growing array of victims

Of course, we do not have to be IT nerds and technology geeks to get caught out by these threats; today everyone has become an IT user (in fact, as more services move online, it is hard not to be one) and so the landscape of possible victims – whether we consider these to be systems, individuals or organisations – has become far more diverse. Meanwhile, however, people have got little better (or maybe no better!) at protecting themselves from other perspectives, and the innate level of security literacy and threat awareness remains low (Furnell and Moore 2014, 12–18). Indeed, cyber-dependent crimes are also ones about which the vast majority of the population have little or no real comprehension. While it is relatively easy to relate to most forms of physical or real-world crime in terms of how and why they happen, the basis from which one might find themselves exposed to hacking or malware is shrouded in mystery for most users, and leads to the ‘why would it happen to me?’ mentality. Most remain unaware that the opportunity to harvest their personal data, or to enlist their computer as a participant in a botnet, makes their system as valid a target as many others. Moreover, if the system is vulnerable to the type of exploit that a given attacker (or
malware) has got within their arsenal, then it makes the system a preferable target to a system that has been better protected.

The exposure is also likely to increase as more systems, applications and devices rely upon us to update them in order to ensure that they remain protected. This is something that we have been pretty poor at doing, even with one or two things to manage, and so the problem is only going to be amplified as there is more technology to be looked after. As an example of previous bad practice in this regard, we can consider the slow and lingering death of Windows XP – an operating system launched in 2001, superseded in 2007, withdrawn from support in April 2014, and yet still in wide scale use well over a year later (with figures in early July 2015 suggesting that it still accounted for around 13 per cent of Windows-based installations, as against only slightly – 17 per cent – using the a version of Windows 8, which was the latest version at the time of writing) (NetMarketShare 2015). The significant risk here is the ongoing exploitability of the systems concerned. Even during its supported lifetime Windows XP was hardly a stranger to vulnerabilities being discovered and exploits being released. As such, it became a routine requirement (at least amongst dutiful system administrators in organisations and diligent end-users at home) to keep the systems regularly patched. Those that were not updated found themselves at far greater risk, both from malware and other forms of online attack. So, as these systems continue to be used beyond the officially declared end-of-life, and no longer receive any ongoing support from Microsoft in terms of security updates, they represent a lingering risk to both their owners and other Internet users who may find themselves indirectly affected as a result (e.g. thanks to a compromised XP system being harnessed into a botnet and sending out spam to all and sundry). Although some might argue that, with such a significant user base still remaining, Microsoft ought to have further extended support, the key requirement here is really for users to be sufficiently aware that their technology poses a risk and be prepared to take action. However, while we have readily adopted the technology, we do not have such an established culture of protecting it.

It does not help when things go from being safe to becoming a danger. Mobile devices are a case in point here, as we have transitioned from basic mobile phones (with limited processing and storage, and a communications capability that typically just covered voice calls and text messaging) to smartphones (with their myriad apps, gigabytes of storage, and always-on broadband data connectivity). We have gone from having very little to worry about aside from the loss or theft of the device itself (in which the main value came from the cost of the hardware) to a point where mobile platforms are now exposed to a whole range of specific threats, with the key value now almost certainly being related to the data/content rather than the physical devices.

These examples highlight the fact that tackling the cybercrime threats requires more than just installing a security technology and expecting the problem to be solved. Potential victims, be they organisations or individuals, need to recognise the routes through which exposure can occur, as well as the fact that something that was safe today could be vulnerable tomorrow. This becomes further apparent when looking at the nature of the threats themselves. As such, the remainder of the discussion in the chapter is focused upon some examples that illustrate this evolution. Rather than attempting to consider all the different manifestations of cybercrime, attention is instead directed towards a specific example of the problem – namely the threat of malicious software, or malware. This is not a difficult choice to make, given that this is typically the one that many people most readily associate with computers, and indeed perhaps best exemplifies the way in which technology has given rise to an offence that was previously without parallel in the traditional crime space.
Malware: the threat that keeps on giving

The problem posed by malicious software – as traditionally represented by viruses, worms, and Trojan horses – provides a good illustration of the changing nature of the cyber-dependent threats. In today’s world, these threats can be readily encountered across many devices and online activities, and so malware is basically an issue about which all users ought to have a level of awareness … and ideally some associated protection.

Of course, malware has been a long-standing problem, posing a growing threat to systems ever since the original PC viruses of the mid-1980s. In the early days they spread primarily via the exchange of removable media (specifically floppy disks), and in many cases the payload effects were fairly innocuous (although infection was still not something that anyone particularly welcomed). As time passed, the techniques evolved and viruses soon found their way to infecting executable programs, documents, and various other carriers in addition to boot sectors in which they had originally concealed themselves on the disks. The most significant development in terms of amplifying the potential impact of the problem was when malware strains emerged that started to leverage our Internet connectivity. Of course, the first network-based malware actually predated this by some years, with the Internet (or Morris) Worm of 1988 representing the first large-scale incident. However, the Internet in 1988 was a very different thing, with only around 60,000 host systems, residing mostly within scientific and educational establishments. By the time that malware harnessed it en masse in the late 1990s, things had changed significantly, with growing public adoption by organisations and home users meaning that there were now millions of systems and users to fall victim. Indeed, this was early evidence that our IT practices would directly influence the nature of the threats – in short, where we go, the malware will follow.

Reading the security surveys of today, malware typically takes the top spot in terms of reported incidents. For example, looking again at the Information Security Breaches Survey series, the detail in Figure 3.1 has already illustrated that it was the most frequently encountered category amongst the cyber-dependent categories. Moreover, in the most recent releases of the survey it was also the most frequently encountered of all breach categories amongst both large and small organisations, placing it ahead of ‘Attacks by an unauthorised outsider’, ‘Theft or fraud involving computers’, and ‘Other incidents caused by staff’. For small businesses in particular, it was significantly ahead of other breach categories, suggesting that while the potential for staff-related incidents and more specific targeting by external attackers may increase with organisation size, the indiscriminate nature of malware can mean that size is far less of a factor. So, while it does not necessarily end up being the most costly category, malware is clearly amongst the most prevalent, and therefore something that organisations would ignore at their peril.

Part of the reason for this prevalence is that malware has managed to find its way to us via every conceivable channel, plus some that we would not naturally expect. As successive online services have proven popular (from email and instant messaging through to social networking and mobile apps), so the malware has followed along and attempted to use them as a channel for infection. Its chances here have often been aided by the fact that public awareness of the threat tends not to keep pace with the reality, and while many users may ultimately have got the message that unsolicited emails and attachments may be unsafe, they may remain totally vulnerable to malware reaching them through an unexpected route such as their social network.

As time has gone on, the malware problem has basically become more problematic in all dimensions:
• The threat has increased in volume. For example, in 2014 Kaspersky Lab reported that it was identifying 325,000 new malicious files per day (Kaspersky Lab 2014a). This represented an increase of 125,000 per day compared to 2012, and is a world apart from 2008, when we were talking in terms of about 500,000 known malware strains in total and 8,000 new ones being discovered per month (and back then at least, even these numbers seemed significant).

• Current malware has a greater degree of sophistication than that of the past. In addition to the technical complexity of the code (as exemplified in landmark cases such as Stuxnet, Duqu and Flame, all of which were noted for their complexity (Kushner 2013)), where malware might once use a specific technique to get into a system and do a specific thing once it got there, today’s malware can employ a multitude of methods and will often just steal everything that is available, and allow the attackers to work out what to do with it later (Lee 2011).

• There is now a greater range of infection routes, meaning that potential victims can encounter the problem through a wider range of services and devices. Gone are the days when malware was just a concern for PCs, or when the most likely way to get it was as an email attachment. It can now reach us across various devices, and via all manner of applications, and more particularly via websites and other online routes if our systems are hosting vulnerabilities that leave them exploitable.

Moreover, all of this has been accompanied by a notable change in the intended behaviours, with today’s malware having more overtly criminal intentions than that of the past. Put another way, many attacks have now gone from being the motive to being the means. Rather than simply releasing malware in order for it to be seen and make a mark through media attention, the end objective is now often an organised criminal activity rather than predominantly the realm of individuals or groups actuating in pursuit of challenge, mischief or other non-financial motives. It also ends up being used in support of state-sponsored attacks, corporate espionage, and as an extension of real-world conflict.

There has also been a significant shift in the participants and their roles. The creator of the malware or exploit code is no longer necessarily going to be the ultimate user, and is often developing it specifically for others to use – often for a fee. This in turn brings the concept of a marketplace, where attacks – both general and targeted – can be bought by those that desire and require them. A good example here is ZeuS, a highly prevalent banking Trojan, which was originally identified in 2007 but became most prominent from 2009 onwards, leading to millions of infected machines in over 190 countries. ZeuS offered a variety of mechanisms for stealing data, including the use of webinjects, which were used to inject rogue content into banking websites (e.g. changing the page from asking for selected login information to asking for full details of the user’s secret information, which would then enable theft from their account later). Such webinjects could be found for sale in online forums, with targets including American, British, Canadian, and German banks, and priced according to the scope of the targets concerned (e.g. the cost of one webinject pack was $60, whereas a UK webinject pack cost $800, and updating or modification of webinjects was $20 each) (Klein 2011). Clearly the ability for attacks to be purchased in this way, by parties that would otherwise not have direct access to them, affects the potential scale of both the problem and the victim base, with attackers having a more specific motive and their targets facing a more specific risk.

A further change, and arguably the most notable one from the victim perspective, is the fact that the malware can now reach us in contexts that were previously immune or unrelated to it. This links to the point about the range of infection routes in the list above, and is particularly
illustrated by the rise of malware on mobile devices such as smartphones. While this threat had long been foreseen by many security professionals, by the time it actually arrived mobile phones were an established technology that millions of people had owned for years, and were accustomed to using without any concern about malware. With this in mind, the change of circumstance is a good example of how the cybercrime landscape can evolve in new directions and catch us out. As such, this is the focus of the penultimate section below.

Mobile malware – an old problem in a new guise

As highlighted by the ITU statistics at the start of the chapter, mobile devices have been the big growth area for IT in global terms, and so following some of the observations from earlier discussion, that alone makes them an attractive target for attack. And, as also mentioned earlier, mobile phones are a technology that have moved from being relatively ‘safe’ in security terms (and completely safe from the perspective of malware) to being an area in which users need to be explicitly aware of the threat and take steps to protect against it. Moreover, this has happened within a very short space of time, with the almost inevitable consequence that those using the technologies have often been caught off-guard. For example, if the numbers are to be believed, then we have gone from a situation where there was an average of over 800 new mobile malware discoveries per month during 2011 (Kaspersky Lab 2013), to an average approaching 5,000 per day just three years later (G DATA 2015).

While there are a variety of mobile devices and operating systems to choose from, they have proven to be far from equal in their attraction to malware writers. Indeed, although various mobile platforms, including Symbian, Windows Mobile and even iOS (or iPhone OS as it was originally called in the pre-iPad days) had been around in the market for some time before, it is Google’s Android operating system that has proven to be by far the most attractive target in this space. The reason for this is based upon two significant factors. Firstly, Android quickly amassed a large user base, running on products from multiple manufacturers, spanning a full spectrum of budget and high-end devices. Secondly, the sources from which users can download apps were not regulated and restricted in the same way as those on some of the other platforms. For example, while Apple operated a walled-garden approach with iOS – only allowing users to download apps from its own App Store, and requiring apps to be submitted to a formal approval process before being made available (which in turn involves some level of code verification in order to guard against malicious content) – the Android approach was far more permissive, with Google Play (formerly the Android Market) allowing open and relatively unrestricted submission of new apps. As a consequence, apps with malicious functionality were able to pass through unchecked, giving them ready access to a large community of potential users; as a result of this, Android was quickly able to develop an unwanted monopoly position in its share of the mobile malware market. Indeed, looking at figures published by Kaspersky Lab in late 2014, 98 per cent of all mobile malware detections during 2013 were on Android (Kaspersky Lab 2014b).

In parallel, however, the awareness of the threat and the accompanying use of malware protection on mobile devices has simply not kept pace. For example, in a survey that we conducted amongst 1,222 users in the UK, the US, Malaysia and South Africa, we discovered that while 91 per cent reported having antivirus protection on their desktop or laptop PCs, only 10 per cent claimed to have similar protection on their phone. Of course, as readers familiar with the market during this period will know, users on iPhones would not have had the option to do so in the first place, as no such apps were actually available. With this in mind, we also looked at antivirus usage amongst the specific subset of respondents that were Android users.
This yielded 688 eligible respondents, but the level of antivirus usage remained very low, with only 14 per cent reporting having it.

This lag between the emergence of new crimes and our awareness and preparedness for them does not bode well for the future. The evidence of the past suggests that we will only see a further broadening of the attack surface – in terms of both devices and services – and so new technological opportunities ought to be approached with more readiness from the outset, rather than recognised retrospectively. Unfortunately, we have yet to see signs that this is the case…

At the time of writing we would appear to be standing on the brink of a new era of problems thanks to the emergence of the Internet of Things and a whole new landscape of online devices. Our drive for technological innovation appears to show a remarkable capacity for ignoring the security lessons of the past. In this respect, the IoT is following the well-trodden path of PCs, wireless networking, mobile devices, with all the attention going towards innovating and deploying the technology, while the risks are given little or no consideration. As such, the devices have significant potential to further increase the breadth of exploitable technologies – and to do so on a large scale. As an example, one can now readily purchase IP-enabled surveillance cameras, promoted as a solution for home security and remote monitoring of other premises. However, many such systems are used with default passwords, meaning that anyone willing to do a tiny bit of research to find out what the default is can tap into the device and watch the video that is being captured (NetworkWorld 2014). It is, of course, somewhat ironic that devices specifically installed to improve security in the physical world should find themselves fundamentally vulnerable to being exploited on the cyber side. However, the same problem has previously been seen with unsecured wireless access points, with devices shipped without security enabled and with default passwords to administer them, and so it is not hard to foresee that a similar potential for misuse would exist here.

Conclusions

Whether or not we agree with their specific categorisation as cyber-dependent crimes, it is clear that the various technology-centric methods of attack have become an increasing threat to the security of our systems and data. The very nature of our technology-dependent society means that this situation is highly unlikely to be reversed. Unfortunately, however, the evolution of these threats is significantly outpacing our ability to recognise and respond to them. Indeed, from a cynical perspective, one of the main advancements over the years appears to be that we have now got more names for the things that can harm us; our ability to protect against them still leaves a lot to be desired.

In reading the chapter, it may have been noted that it has devoted little attention to describing the specific workings of the malware or other attacks. The basic reason is that, if we have an eye to the future, many of these underlying details do not matter. The specifics will change, and will depend upon the technologies and opportunities of the day. What is notable is the broader trend towards greater exploitation and sophistication. And what is therefore important is to realise that the only way to manage the situation is through ongoing vigilance. Old threats will persist for as long as the opportunity exists to use them, and new ones will emerge where fresh opportunities can be found. Meanwhile, criminal activities will continue to be drawn towards whatever openings the technology can offer – and this tends to follow the technologies that we ourselves find the most attractive for our own reasons. As such, we need to recognise that the attackers are on the journey with us, and take steps to ensure that they cannot enjoy the ride at our expense.
Notes

1 First appearing in September 2013, CryptoLocker was PC-based cryptoware/ransomware that encrypted the contents of the user’s drive(s) and demanded payment in order to get the decryption key. Over half a million computers were reportedly infected with it between September 2013 and May 2014, with FBI estimates in June 2014 suggesting that $27 million had been paid out by victims in order to recover their data.

2 In addition to being taken from established survey series, the three selected examples present perspectives from the United States, the United Kingdom, and a global sample group.

3 For example, while malware infection was actually the most commonly encountered incident in the 2015 survey (with 84 per cent of respondents reporting it), only 11 per cent considered it to have been the cause of their worst security incident. By contrast, a third attributed their worst incident to a category not shown in Figure 3.1, namely ‘Theft or unauthorised disclosure of confidential information’ – which could arguably result from deliberate cyber-enabled or cyber-dependent attacks, or indeed from accidental incidents.

4 The first reported example was the MS-DOS-based Brain virus in January 1986. In this case the payload effect was essentially harmless, simply changing the name of the disk (the volume label) to become “©Brain”.

5 Written as an experiment by Cornell University student Robert Morris, the Internet Worm spread far faster than he had intended, and quickly ended up infecting around 10 per cent of the hosts on the entire Internet. Moreover, the volume of traffic that these systems then generated, as the worm sought to find other systems to infect, served to bring the network to a standstill. The incident was the direct catalyst for the formation of CERT – the Computer Emergency Response Team – in order to ensure that the growing Internet community was ready to deal with such incidents in the future.

6 The data was collected in different phases, collectively spanning the period between September 2013 and November 2014.

7 The background here is that because App Store content is subject to verification before it is approved for release, this is considered to remove (or at least minimize) the potential for malware to slip through and find its way onto user devices. With this safeguard implicitly providing protection by default, Apple does not see a valid market for antivirus tools and does not approve them for inclusion in the App Store. There is, however, a risk for users that have chosen to jailbreak their iPhone/iPad, in order to enable apps to be installed from non-approved sources. In these cases, malware has a route onto the device, and may exploit the additional access rights that jailbreaking will have made available.

References


