WALKING IN NO-MAN'S LAND

Beyond Asimov's laws of robotics: sleepwalking toward the future?
Irakli Beridze and Odhran James McCarthy

Virtual currencies: safe for business and consumers or just for criminals?
Erik R. Barnett

Securing justice for survivors of conflict-related sexual violence: the stigma belongs with the perpetrator
Zainab Hafsa Bangura
Freedom From Fear Magazine
Special Edition including a limited selection of articles from this year’s issues

Walking in no-man’s land

freedomfromfearmagazine.org
f3@unicri.it
unicri.it
Nobody’s going to fix the world for us, but working together, making use of technological innovations and human communities alike, we might just be able to fix it ourselves.

Jamais Cascio
Editorial Board
UNICRI
Jonathan Lucas
Marina Mazzini

Max-Planck Institute
Hans-Jörg Albrecht
Ulrike Auerbach
Michael Kilchling

Editorial Team
Fabrizio De Rosa
Marina Mazzini
Maina Skarner
Valentina Vitali

Graphic and layout
Beniamino Garrone

Website designer
Davide Dal Farra

Disclaimer
The views expressed are those of the authors and do not necessarily reflect the views and positions of the United Nations. Authors are not responsible for the use that might be made of the information contained in this publication.
Contents of the publication may be quoted or reproduced, provided that the source of information is acknowledged.
The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations and UNICRI, concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.
The mention of specific institutions, companies or of certain manufacturers’ products does not imply that they are endorsed or recommended by the Secretariat of the United Nations or UNICRI in preference to others of a similar nature that are not mentioned.

Photographers
Reportage
Antonello Zappadu

UN Photo

Flickr
Marufish, Simon & His Camera, Exeter Fredly, Thomas Hobbs, Erin Pettigrew, Arkangel, scottks, Francis Storr, M Trombone, astonishme

Other:
IFAD, NASA
New opportunities from globalization

Unprecedented globalization, expansion and change is irrevocably altering global dynamics. Technological evolution has brought about unparalleled levels of progress which continually restructure the fabric of our society, beginning from the very way we interface with one another. Indeed, the achievements of a fast-evolving and increasingly interconnected world with a quantum jump in technology in different sectors benefit mankind as a whole.

We live in a world where the concept of borders has changed radically: there is a growing movement of people, commodities, services and ideas between countries and regions in a common global market. Some clear discrepancies are however surfacing, particularly the gap between the expectations from the future we envisage and are striving for and the stark reality facing many people on a daily basis. New vulnerabilities are emerging, particularly the increasing risk of exploitation of new opportunities for progress by organized criminal networks. Examples of this trend is the exploitation of the benefits and opportunities of cyber-space through cyber crime and the ruthless undermining of State institutions through corruption at all levels.

The very same technology that is providing us with the tools to safeguard freedom of speech providing us the means for instantaneous global communication and free movement of ideas and knowledge is also being used by criminals who phish for individuals private information, credit card details, or who use cyber space as a platform to exchange inappropriate images or sell illegal materials. In response to this, UNICRI has been focusing on cybercrime for many years, enabling the Institute to accumulate the skills and know-how to analyze the many trends associated with online criminal activity. Through its advocacy role UNICRI has contributed to raising understanding and awareness of cyber threats, in assisting law enforcement and policy makers at the national and international levels to address and combat the growing threats to cyber security.

This issue of F3 highlights the importance of involving citizens and their governments in the process of change and to be cognizant to the potential threats to development emanating from their exploitation by organized crime networks. Care should also be taken so that new technological developments do not contribute to accentuating disparities, such as the “digital divide”, but rather contribute to a homogenous and collective growth and collective mutual benefits.
Dossier

Beyond Asimov’s laws of robotics: sleepwalking toward the future?
Irakli Beridze and Odhran James McCarthy

Deep Web, going beneath the surface
Carola Frediani

Are cyber criminals competing at the Olympics?
Alan Brill and Snezana Petreska

Virtual currencies: safe for business and consumers or just for criminals?
Erik R. Barnett

F3 - Young

Uniting beyond borders
Hana Abul Husn

Parallel cities: Buenos Aires’ villas miseria
Carlo Francardo

Main

Finding justice within climate change actions
Brian Harding

Infocus

A matter of justice: protecting land rights for inclusive growth in Africa
Harold Liversage

Photo

Photo reportage
Antonello Zappadu
ARE CYBER CRIMINALS COMPETING AT THE OLYMPICS?

By Alan Brill and Snezana Petreska

Mass gatherings of cyber connected people are magnets for predatory cyber criminals

Events like the 2014 World Cup and the 2016 Summer Olympic Games (both of which are being held in Brazil) as well as national and regional events can draw tens of thousands or even hundreds of thousands of fans. Cultural events like concerts at arenas and sports stadiums can result in masses of viewers. While we think of these mass events and the joy and excitement associated with attendance at the games, concerts, conferences, or gatherings, those in the criminal justice field clearly recognize the potential of these events to have an opposite effect by attracting criminals – who may engage in petty or more violent crimes – or terrorists. Law enforcement teams would be looking at the risks of explosive
devices as well as at chemical, biological or radiological weapons of mass destruction. But there is a far more likely risk that is associated with these events, and it is a risk which can be easily overlooked — targeting of attendees by cyber criminals. The opportunities for cyber crime are endless, the technology to carry it out is readily available, the targets are often unaware of the risk, and in many cases have little or no effective defense. Major events generate an environment in which creative cyber criminals can thrive. In effect, the cyber criminals can compete in their own games for money, information and even for bragging rights on their status as a wizard among hackers.

The opportunities for cyber crime are endless, the technology to carry it out is readily available, the targets are often unaware of the risk

Why Target Mass Events?

Today, most large-scale intrusions into computers and networks can be classified as looking for money or opportunities that can be turned into money — like identity information, credit card information, or proprietary information (like unreleased financial data, “insider” data or trade secrets). There are also cyber attacks that are designed to punish a company or government agency for some action they took (or didn’t take) through denial of service attacks, website defacement or the release or sensitive or embarrassing information. These may be carried out by adversaries (competitors) or by governments (or those they covertly sponsor) or even by hackers who have an ideological objective (sometimes called “hacktivists”). The hacktivist’s objective is to cause some form of reputational damage to the organization. But what are the motives that would result in significant numbers of cyber criminals (and in some cases intelligence organizations) focusing their attention on large-scale sporting, cultural or political events? We have identified five key factors:

The cyber criminals can compete in their own games for money, information and even for bragging rights on their status as a wizard among hackers

- A Target-Rich Environment.

It’s obvious that these events draw crowds ranging from tens of thousands to hundreds of thousands of attendees. But it is not simply the numbers; it is the evolution of technology that makes these gatherings such good places for hackers to insinuate themselves. We are the most “connected” generation in history. In a very few years, we have gone from using notebook computers to relying on tablets and even more on smartphones. These mobile devices have become globally ubiquitous. Look at photos of groups of people at events, and you will undoubtedly see a fair proportion of them holding or using smartphones. They may be telling people what they are doing, perhaps through text messaging or blogging. They may be taking photographs, either of the event, or of themselves and instantaneously posting them on the Internet. Indeed, the word “selfie” meaning a photograph you take of yourself (generally with a smartphone or tab-

---

1. Be aware, however, that in some cases, cyber criminals or state-sponsored actors can carry out a denial of service or web defacement attack as a way of diverting attention from a simultaneous attack designed to penetrate the target’s defenses and to exfiltrate data, cause destruction or to implant a “back door” to facilitate future access. Organizations that suffer a denial of service or similar attack should recognize this issue and take steps to determine if a parallel attack is attempted or has been successfully carried out.
let) that you share on social media was named Word of the Year 2013 by the Oxford Dictionaries. People are using their mobile devices (and more traditional laptop computers) to keep in touch via electronic mail, to communicate over social networks and to send and receive text messages, but increasingly, they are performing financial transactions and working remotely which often involves accessing valuable intellectual property. At locations around event venues, visitors are connecting to WiFi networks operated by hotels, coffee shops, fast-food restaurants and other establishments. The reality is that having lots of people connecting to lots of unfamiliar networks to conduct sensitive transactions on machines that often store highly confidential information is a dream come true for the cyber criminal, the state-sponsored actor, and the hacktivist. In Brazil, about 40% of the population is online. Brazil also has one of the world’s largest computer and mobile technology market, social media communities, and e-commerce platforms. It is a hot spot for cyber criminals and it also is home to some of the most notorious hacking groups. Notably, BMPC, a Brazilian hackers group, is known for the cyber attacks against NASA. In 2011, LulzSec, another Brazilian hackers group, launched attacks against government websites, including the website of the President. The hackers of Anonymous Brasil, a self-proclaimed faction of the

---

4. According to a report from the consulting company Kleiner, Perkins, Caufield and Byers, the Brazilian market is the fourth world’s biggest IT market [http://www.kpcb.com/internet-trends](http://www.kpcb.com/internet-trends)
Anonymous hacktivist group, in 2012 launched Distributed Denial of Service (DDoS) attacks against three leading banks in Brazil, and has been openly expressing its opposition to the 2014 World Cup. In 2013 the Confederations Cup in Brazil attracted 250,000 foreign visitors and the World Cup 2014 attracted approximately 1,000,000 foreign visitors. This high concentration of potential victims was not unnoticed by cyber criminals who are likely to make the most out of the opportunity to get access to private information of the many foreigners who otherwise would be out of reach. These foreigners, in addition, were likely to return home quickly, and would be unlikely to return to Brazil to be a part of prosecuting a cyber crime. During the 2012 United Nations Conference in Rio de Janeiro, the Brazilian government identified 140 attempted security breaches. During last year’s Confederations Cup in Brazil, the numbers were even higher.

We are the most “connected” generation in history. In a very few years, we have gone from using notebook computers to relying on tablets and even more on smartphones

- A Trusting Target Audience.

When you are at a mass event, be it the Olympics or a huge concert by a rock and roll legend that you have been waiting years to see, the reality is that being a target of a cyber security attack is not top of mind. Generation Y has grown up online, and largely expects connectivity to be available where they are, when they want it, and affordable, if not free. When traveling, many people are glad to be able to connect to a WiFi signal at an airport, hotel or coffee shop. In many cases, these are open networks that do not require prior authorization or authentication. By design, many schools, universities, libraries and other facilities provide ubiquitous internet availability to all, whether guest, student, faculty, or casual visitor. And once connected to the network through a smartphone, tablet or laptop computer, many people set their devices to connect automatically in the future with no action required on the part of the user. People tend to not think of the risks associated with being on public networks. While there may be warnings, either provided on an initial screen or by the operating system of the device being used, most people simply click through to establish connectivity. Issues like site spoofing and false flagging (which will be covered below) are also not top-of-mind and this can lead to many problems. Another user-related vulnerability is that often, in spite of awareness training, users still fall for social engineering scams. They may believe that they have received an urgent email from their boss or from their company’s human resources department. They may receive an email telling them that they have won an international lottery (even though they know they never entered such a contest) or will be paid a fee (for example, by the widow of the late leader of some country) to help move huge sums into various bank accounts. In some of these cases, the recipient is being targeted for either a payment (of a required “bank fee” or “facilitation fee”) or for their banking information (which will inevitably result in their account being looted). In other cases, the target is asked to click on either an attachment or a link that will tell the person exactly what they need to do to get not only the money promised, but a bonus as well. Unfortu-

9. The statistic provided by the Centre for Cyber Defense, an institution which is part of the Brazilian Army, was widely reported in mainstream media: http://m.folha.uol.com.br/mercado/1043519-apos-bc-hackers-atacam-sites-de-mais-tres-bancos-nesta-sexta.html
nately, all that the person gets from the attachment or the hyperlinked file is infection with one or more pieces of malware. Some of the malware simply steals data. Other malware may encrypt files on the computer’s storage devices and provide a demand for ransom to be paid to get the key for decryption of the files. Even if the ransom demand is met with a payment, there is no guarantee that a code to actually decrypt the data will be forthcoming. And there is a fairly high likelihood that the so-called “ransomware” infection may well have been accompanied with automatic downloads of other malware, which may continue to run (and steal information) even if the ransomware is successfully destroyed or inactivated. It can be the gift that keeps on giving (to the bad guys). Fans and visitors of the World Cup and the Olympics are considered easy targets by hackers. The most common technique used by hackers to steal data or gain access to confidential information in Brazil is phishing, where seemingly innocuous electronic communications prompt victims to follow a link to a fraudulent website to enter banking credentials or download malicious software that sends out sensitive data. Kaspersky, one of the leading providers of internet security solutions for end users, claims to have been blocking 40 to 50 fraudulent websites related to the World Cup every day, in Brazil alone. In addition to phishing emails, social media is used extensively by hackers in Brazil, given the widespread presence of Brazilians in social media. Hackers inject malicious links to posts in popular legitimate social media forums, and direct users to malicious websites. The recent statistics are alarming as well. In 2013, approximately 22 million Brazilians were victims of cybercrime. This represents approximately 10% of the population. The estimated cost of these crimes was more than R$18 million. In the month leading to the 2014 World Cup (May 19 – June 19, 2014), Kaspersky Lab Technology reported to have blocked 87,776 attempts to launch malicious programs in Brazil, a significant jump from prior months. This number is four times higher than Russia’s, ranked second on the list.

During the 2012 United Nations Conference in Rio de Janeiro, the Brazilian government identified 140 attempted security breaches.

- A General Low-Level of Security

If we ask typical business computer users whether malware detection software resides on an employer-provided laptop or desktop computer, it is very likely that the vast majority of them would say “of course”. Similarly, if we ask if you have similar software on your personally-owned PC or Mac computer, we think most readers would say “yes”. But if we were to ask whether you had installed anti-malware software on your tablet, or particularly on your smartphone, the answer is likely to be that you did not. That is unfortunate because whether a phone uses Android, IOS or another operating system, it is vulnerable to malware. Corporations know this, and often install and maintain special software (called “mobile device management” or “MDM” software) that can protect corporate information on the device, but many individuals ignore the issue and do not know whether their device is actually protected or not. Even where we are dealing with the more traditional laptop computer, there can be issues. For example, millions of computers still run Microsoft’s Windows XP operating system, even though that operating system is no longer supported and as a result, Microsoft does not publish regu-

---

13. It is possible that in some cases, anti-malware software could have been installed by an employer (for employer-supplied phones), or by a cellular carrier, without the knowledge of the end-user. But given the risk, we believe that smartphone users need to actually know whether this software is installed or not. “Assuming” that it is installed is not enough. You need to know whether it is in place and active, or not.
lar updates (patches) to deal with security issues identified after the official end-date for XP support, which was April 8, 2014. Without such updates, vulnerabilities identified by hackers affecting the XP platform will likely remain open security issues as long as XP continues to be used. What this means is that many devices that would likely be in use by those traveling to see major sporting, cultural or political events may be running systems with known weaknesses in security. There is little question that exploitation of such weaknesses are among the most important ways through which adversaries gain access to devices and through them, to networks. In Brazil, the rapid development and implementation of internet connectivity and electronic activity has not been mirrored by the implementation of cyber security legislation or security practices. Brazilians are generally not common users of internet security protection software and many internet users lack basic cyber security knowledge. Moreover, in Brazil there is widespread use of pirated software. Pirated software tends to leave users vulnerable to experienced hackers because of its inability to receive security updates to protect from the latest vulnerabilities. Internet cafes and the numerous hotspots on open systems further provide hackers with the opportunity to exploit the lax security environment making easy targets of visitors from around the world using unsafe devices.

People tend to not think of the risks associated with being on public networks

- The Availability of Technology to Support Cyber Crime
  In the past, carrying out cyber crimes often required a high level of knowledge and very sophisticated equipment. This is no longer true. Simple-to-use devices that are readily available on the open market are all that is needed for this type of crime. For example, to set up a fake “hotel” WiFi system takes only a device that connects the perpetrator’s laptop to a cell phone data network and a wireless access point that generates the fake “hotel” WiFi network. The software is also immediately available. Hence, the number of potential perpetrators is immense. Add to that the fact that thefts of this type are often carried out by organized criminal enterprises that can provide their individual “workers” with precisely the hardware, software and instructions necessary to carry out these frauds. This creates a monster-sized problem that goes far beyond issues relating to travelers’ computers, tablets and smartphones. The actual work is minimal. Choose a location, establish your connection to the Internet, run the software to establish your WiFi presence in the targeted location, and the software does the rest. It can record all of the non-encrypted traffic on the network; it can, in some cases, load malware onto victim’s machines that connect to it if they have certain vulnerabilities. The information is collected and can be harvested either on the spot, or by holding the captured information for analysis - and exploitation - at a later date. What is perhaps more insidious is that another objective of cyber criminals is to install malware. Current malware is very dangerous and very powerful. Worse is the ease with which this can be deployed. Once, perpetrating a cyber crime actually required significant skills. This is no longer the case. Would-be cyber criminals now need only to purchase the malware kit and instructions for using it. In a recent international police action coordinated by the European Union’s Eurojust agency, law enforcement officials in 16 countries conducted raids and made 90 arrests of individuals who developed, distributed or used a particular form of malware known as BlackShades. Thousands of people bought the malware – some for as little as US$40. BlackShades is a particularly insidious piece of malware. The capabilities of this malware were described as follows by the European Police Agency, Europol:

14. While the XP operating system continues to have vulnerabilities, several government agencies are paying Microsoft to develop and distribute (to them only) security updates. In addition, some computer environments include software that will only run on an XP platform. These systems need specialized protection, such as isolating the machine from the Internet.
BlackShades has sold and distributed malicious software (malware) to thousands of individuals throughout the world. BlackShades’ flagship product was the BlackShades RAT, a sophisticated piece of malware that enables its users to remotely and surreptitiously gain complete control over a victim’s computer. Once installed on a victim’s computer, a user of the RAT is free to, among other things, access and view documents, photographs and other files, record all of the keystrokes entered and even activate the webcam on the victim’s computer – all of which could be done without the victim’s knowledge. BlackShades also makes it possible to carry out large-scale distributed denial-of-service (DDoS) cyber attacks. A particularly malicious aspect of this software is the ability to encrypt and deny access to files.\[^{16}\]

The recent statistics are alarming as well. In 2013, approximately 22 million Brazilians were victims of cybercrime. This represents approximately 10% of the population.

While there are literally thousands of persons who have purchased the malware who were not among

---

those arrested, it is highly likely that the major vendors of anti-malware software will quickly devise ways to detect and deal with this software. The availability of this malware, with this range of capabilities and ease of use, at such a low price point should serve as a warning to all that the tools needed to conduct effective hacking are readily available. It should also be remembered that the risks associated with large events like Olympic Games do not end when the event ends. If a piece of malware can be inserted into a machine during the games, it may go on to infect the machine - or, perhaps any network it is plugged into back at home or at one’s office - and continue to exfiltrate data or permit unauthorized access for extended periods.

Pirated software tends to leave users vulnerable to experienced hackers because of its inability to receive security updates to protect from the latest vulnerabilities

• The Low Likelihood of Immediate Arrest or Interdiction
The recent coordinated raids and arrests in conjunction with the development, sale and use of the BlackShades software (discussed above) is, unfortunately, the exception to the rule. Coordinating multinational police actions takes time and resources. In most cases, any action would be local or national in nature, and even there, because of a lack of resources, most malware incidents will never result in a prosecution. In fact, there are substantial statistics that show that in many cases, the cyber attack is not even noticed by the attack victim for a long time. One recent study of cyber intrusions indicated that the average time between the actual intrusion and the beginning of data theft (actual exfiltration of data) is measured in minutes or hours, while the time between the intrusion and the company noticing that it has been attacked is measured in weeks, months and sometimes years. In one of our cases, a company was notified by the FBI that their network had been compromised by state-sponsored actors, and that it had been happening (completely unnoticed by the victim company) for more than two years. All in all, the chances of being caught and punished are very limited.

To set up a fake “hotel” WiFi system takes only a device that connects the perpetrator’s laptop to a cell phone data network and a wireless access point that generates the fake “hotel” WiFi network

• The Anatomy of a Mass Event Cyber Crime
Cyber criminals understand what traveling businesspeople do to gain connectivity in hotels, airports, restaurants, arenas and other venues. Their job is to make what they are doing part of the landscape, so that you do not even see them. Here are some of their favorite methodologies.

  > Wireless Interception
When you connect to the Internet via WiFi, you have to remember that you - and everyone connected to WiFi - are actually transmitting radio signals. Unless the signal is encrypted, anyone in range can intercept those signals and read them. Since many hotel and coffee shop WiFi spots are not encrypted, this interception is easy to do.
> **False-Flagging of WiFi**
Another way to gain access to your data is to set up a WiFi site that seems to be the one your target user is looking for. For example, if you are staying in the ABC hotel, you might find a WiFi site named “ABC Free WiFi” but it might actually be run by a hacker. When you connect, you might well see a sign-on screen that asks for your name and room number to “authenticate” you, but the objective is to steal your data and, in some cases, to download malware to your computer to permit ongoing access.

> **Water Hole**
One of the favorite tricks of the hackers is to compromise a website that they know their target audience will visit. It could be one that had (or at least purported to have) inside information on the event one plans to attend or visit or other useful information. The hackers then reconfigure the site’s code to download malware into your system, enabling them to take control of your computer, or at least to harvest information from it. This is called a “watering hole” attack in that it is similar to poisoning an animal watering hole to attack all of the animals that visit for a drink. Hackers may attempt to turn legitimate or counterfeit FIFA, or Olympics-related websites, into watering holes in order to target the wider potential audience. Additionally, legitimate social media websites can also be turned into watering holes, or at least to direct the unwary to watering hole sites. Brazil is Facebook’s second largest market, and Brazilians use social media as one of the main ways of communicating. Because legitimate sites can be “hijacked” by criminals who can manipulate the Internet’s Domain Name System (DNS) to direct traffic from the actual site you are trying to reach to their fake site, there is no perfect way to protect yourself. The only defense is to only visit sites that you regularly use and know to be legitimate, recognize unusual changes in those sites, have absolutely updated anti-malware protection, and to limit the sensitive information that you carry on your portable device or access through it. Even following these precautions might not provide absolute safety.

> **Compromising Wired Systems**
Many people feel that using a wired connection in a hotel eliminates the malware risk. That is just not true. Anyone who is able to plug into the same part of the network – like in a nearby room – can often compromise your computer. On the wired connection, all of the packets that make up our messages have an address which identifies the computer to which the packet is addressed. But it is easy for a hacker to read all of the packets and to re-assemble them into messages. Interestingly, a computer that is reading every packet - as opposed to one that is only reading its own packets - is referred to as operating in “promiscuous mode.” The lesson is that if your messages are not encrypted, they are at huge risk of being compromised.

> **Physical Access to Target Computers**
Traveling executives often need to leave their computers in the hotel room when they go to dinner, or to places where they do not want to carry a computer. Most understand that leaving their computer sitting in their hotel room is not very secure. So they put it in the in-room safe. Today, almost all of these safes are digital - you put in a 4 to 6 digit code to lock the safe, and the same number to open it. Of course, the hotel has to have the ability to open the safe (for example, if a guest leaves it locked or “forgot” the code). This usually requires plugging in a device (which may be a special device or an app on a smartphone) that will unlock the safe. One safeguard, according to hotels, is that the room

door lock generally records the card that opened it (so that they can tell if your door was
opened by a housekeeping key, for example) and that often the halls are monitored by sur-
veillance cameras. While all of this is true, hotel safes are regularly opened and contents
stolen. Consider that if an insider at the hotel is colluded with hackers, they could open
the door, open the safe, allow the hackers to copy the contents of the computer hard drive,
and re-lock everything. If you do not know there had been an intrusion, there would be
no complaint, the evidence would never be examined, and would eventually be discarded.

> Theft of Computers

Another way of gaining access to information on a computer is to simply steal the de-
vice itself. We have clients reporting thefts from hotel rooms, from offices they are vis-
iting where the computer “disappears” overnight, and even one case involving three
American consultants visiting São Paulo who were in a car stuck in a huge traffic jam
on an elevated highway. They were all working on their computers while commuting
to their hotel. Two motorcycles, navigating between lanes of cars, stopped on either
side of their car. The motorcycle drivers produced pistols, pointed them at the consul-
tants, and collected their computers, which they shoved into their backpacks. They then
drove between the lanes of stopped vehicles and disappeared down the next exit ramp.

> Theft of laptops and mobile devices is common around mega events.

Especially in Brazil, theft of laptops has been prevalent. As with the example above, it com-
monly occurs in the form of armed robberies of passengers while they are sitting in their
cars or in lobbies of hotels, or when computers are left briefly unattended. Theft of smart
phones is similarly prevalent.

What is perhaps more insidious is that another objec-
tive of cyber criminals is to install malware

What can you do? Action Plans for Governments, Corporations and Individuals

There are no perfect solutions. We believe that the best that can be reasonably done is to make sure that
your traveling executives and employees understand the risks, have the tools to protect themselves, and
know how to use them. Collectively these will reduce your risk.

> Encrypt the Computer

The first step you should take is to put full encryption on your portable devices. If your
storage drive (whether it’s a hard disk or a diskless solid-state drive) is not encrypted, it
can be copied. Putting into place any of the full-disk encryption systems will materially
increase your security. Of course, you have to choose a strong password. Also, make sure
you learn exactly when the encryption system is activated. With some packages, just closing
the screen of the laptop will not invoke encryption. You may need to shut down the ma-
chine. Find out how the encryption package installed on your computer works. For smart-
phones, this encryption is often provided as part of a corporate Mobile Device Management
system that may be provided by an employer. For laptops, there are a number of effective
encryption packages that should be provided by an employer or the user of the device.18

18. Note that in some cases, where an employer has a mobile device security plan, there may be a prohibition against an
employee installing their own encryption software (to protect the employer’s ability to access information). But where it is
not present, we recommend talking to the employer about it. For personally owned and used equipment, the owner of the
machine has the responsibility to protect the device and the data stored on it.
Don’t Take Data You Don’t Need
One of the simple rules that many people forget is that thieves can not steal something that is not there. Some executives keep massive amounts of sensitive company information on their portable computers, and when they travel, this information is at risk. The solution is to not carry information that you do not need when you travel. Some of our clients have “travel computers” including only the information they will need for a specific trip, and nothing else. If you decide to transfer information to another storage device (on a network, for example) do not forget that unless you use a program to overwrite the space where it was stored, hackers who can gain access to your computer and can copy the storage drive may be able to “un-erase” deleted files. When returning, have the computer analyzed to determine if it has picked up malware or any kind of unexpected file. We often recommend that the files are extracted from the machine, the machine then wiped and a standard working environment re-installed.

The risks associated with large events like Olympic Games do not end when the event ends

> Don’t Store Any Data on the Computer
A more extreme (but very do-able) version of data minimization is simply to configure your portable computer so that it has no data on it. The programs you need are there, but all data (including drafts and temporary files) are stored on an external memory stick or memory card. SD cards can store 64 gigabytes on a device about the size of a postage stamp that can easily be carried in your pocket or purse. USB memory sticks can have even greater capacities. You carry the storage device with you so that even if criminals access or steal your computer they get no data. Like hard drives, memory sticks can and should be encrypted to protect the data in the event the USB device is lost or stolen. In some cases, an alternative is to store your data as encrypted files in remote (cloud) storage systems accessible via the Internet. Accessing these remote storage systems should be done through a Virtual Private Network as an additional layer of protection, as discussed below.

> Encrypt Data That You are Going to Transmit or Receive
If you have to send or receive files, they should be transmitted as encrypted. Something as simple as an open source encryption system (which can also encrypt all or part of your hard drive) may be the right solution for you.19 File encryption systems enable you to encrypt a file and transmit it. You provide the password for the file in a separate communication to the recipient. This should be done using a means other than that used to send the file. “Out of band” transmissions are for instance considered more secure since it would be necessary to compromise both the transmission of the file and the password in order to access it.

One of the simple rules that many people forget is that thieves can not steal something that is not there

> Go Virtual Private Network - VPN - Immediately and Always
A VPN is a technology that creates an encrypted tunnel between your computer and a remote server. Many companies provide this technology to employees, but some do not.

---

19. Of course, corporate/government regulations, individual hardware/software configurations and specific needs will determine which encryption solution is appropriate in any individual case.
Make no mistake about it. If you are connecting to the Internet from any kind of public network, you need to immediately start a VPN connection. Unless you have a VPN, whatever you transmit or receive that is not encrypted, there is a serious risk of compromising your data. There are many reliable VPN services available, some offering basic services at no cost; most provide good services for less than US$100 per year. Investigate these options and select one that is well reviewed and that matches your needs.

> **Password Protect Your Computer**
You should put a password on your computer so that it can not just be started and accessed. This can be bypassed (for example, by copying the entire hard drive) or, in some cases, defeated using well-known work-around. An example: it was only a matter of days between the release of the iPhone fingerprint sensor and the publication of a work-around to defeat it. Nevertheless, it is considered a basic control and should be put in place.

> **Practice Safe and Smart Computing**
In our work, we analyze computers that have been compromised. We find that in many cases, those using them have succumbed to phishing emails, or visited sites that download malware to visitors’ computers. Only visit trusted and legitimate sites using secure networks.

> **Assume You Will be Attacked**
The single most important thing you can do is to recognize the risk. Work with your IT staff or professionals you trust to build a layered series of protections. For example, you might combine
  » Password Protection
  » Full-Disk Encryption
  » Keeping all data on an external device
  » Immediately starting up a VPN when going on-line.

As we’ve pointed out, there is no such thing as 100% protection. Faithless executives or employees can deliberately take actions to steal data. Security advice and some security systems can be shut off or uninstalled. But taking these steps will minimize those risks. Travelling to any large scale event is going to increase risk. The various protective measures we have outlined, particularly when combined, are going to mitigate your risk and that of your company. Don’t make it easy for the hackers and cyber criminals!

**Don’t make it easy for the hackers and cyber criminals!**

---

**The author**

**Alan Brill** is Senior Managing Director, Kroll, Cyber Security & Investigations, Secaucus NJ USA (E-Mail: abrill@kroll.com)

**Snezana Petreska** is Managing Director, Kroll, Investigations & Disputes, Sao Paulo Brazil (E-Mail: spetreska@kroll.com)

---

20. However, recognize that the computer of someone you trust may itself be compromised and used to transmit email to everyone on the victim’s email list urging them to visit a website that is serving as what is called a “watering hole” which will attempt to download malware to every computer that visits the site.