GUNNAR's BASIC INTERNET SECURITY GUIDE

FIRST EDITION

GUNNAR K. A. NJALSSON

CREATESPACE INDEPENDENT PUBLISHING PLATFORM
AN AMAZON.COM COMPANY

ISNI 0000 0000 7267 1672
VIAF 43702923

THE SPACEPOL CORPORATION is a high-knowledge enterprise with expertise in the fields of public technology policy, space law and comparative national innovation strategy.

GUNNAR K. A. NJALSSON is a graduate of the University of Helsinki and an expert in public technology policy and national innovation policy planning. He has also studied and worked with software engineering and corporate data system planning.

More Information:
www.spacepol.ca
www.spco.eu

ISBN
978-0-9812475-9-5

OVERVIEW OF CONTENTS

INTRODUCTION

THE purpose of this guide is to provide the global corporate internet community with a plain-language warning and source of suggestions to help improve the current state of internet security and decrease the ability of governments and competing businesses to engage in industrial espionage. It is not a complete guide. It is not to be viewed as concrete advice for policy in the case of individual businesses. It is not legal advice.

The guide is aimed primarily at a European, Russian and Latin American audience and expresses opinions from that vantage point. Concretely, the point of departure is that European, Russian and Latin American businesses have every right to protect themselves from privacy violations and spying in accordance with the legislation of their sovereign nations. The guide has been written in light of recent media publicity which indicates that countries such as the United States and the United Kingdom are actively involved in monitoring and surveillance which is directed against the ordinary citizens, businesses and political representatives of sovereign nations. The subsequent lull in the public discussion and political debate about these violations illustrates the need for the internet community in these nations to organize its own counter-measures and methods of protection.

The information provided here should assist corporations and agencies in properly considering important aspects central to the protection of their information assets. The guide will in any case greatly assist organizations in posing the “right” questions when planning internet and data security. While the issues presented here will be touched upon briefly and in a very general nature, it is important that the reader turn to an expert for more detailed advice about a particular issue brought forth in this guide. The SPACEPOL Corporation through its consulting arm, SPACEPOL Government Policy Consulting, provides such consulting services to governments and organizations. The author is a keynote speaker on the subjects touched upon in the guide.

This is the first edition of *Gunnar's Basic Internet Security Guide* and includes nine sections. Subsequent to this introduction, each section deals with a major issue which our expert experience in the field has shown to be a major area of security vulnerability. Most agencies and organizations will be exposed to government and non-government espionage through one or more of these

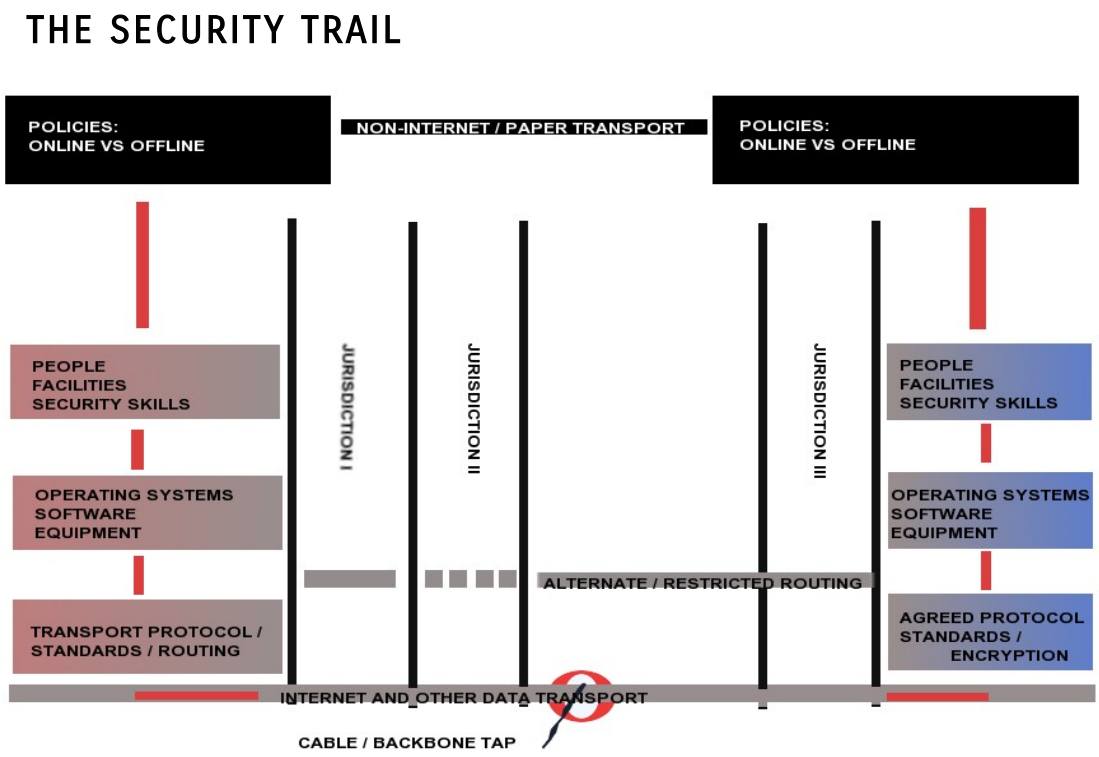
areas of vulnerability. If your organization has not even considered one or more of the issues brought forth in this guide, then it is likely exposed to exploits or violations of data security related to that area. There may not have been any detected security incidents just yet, but the organization may be open to future incidents or past incidents may not yet have been detected or exposed.

Hopefully you will have some benefit from this guide. It is a work in progress and your constructive feedback for making the guide even more useful is always appreciated. Visit the web site of SPACEPOL Academic Publishers and send us a note if you find this guide useful or wish to see it improved in future editions.

THE SECURITY TRAIL

TRACING your data assets from origin to destination is a basic exercise for planning security. The various points along the route from origin to destination, from sender to receiver and user, comprise what can be referred to as "the security trail". The security and legal regime of your data assets at *each point* along the security trail should be the subject of deliberation in your organization.

Who handles sensitive data? How and where are the data stored at your physical location? Is the device upon which they are stored connected to the outside world? What is the legal regime of the physical location of origin and storage of the data? What is the legal regime of the various jurisdictions through which the data will pass and at the ultimate destination of the data? How are the data stored, protected and handled at the destination? Will the data be further released from that facility? Who has access to or control of the data along each point? These are typical basic questions which should arise during your deliberations on the security trail of your data assets.



The figure above is a vastly simplified representation of the security trail and shows two organizations which send and receive data assets from each other. They can do this by traditional means, including paper, non-internet transport of information by choosing to transfer data wholly or in part through controlled physical means. They can also choose to transfer data assets by internet and other forms of electronic data transport such as direct OSI (open systems integration model) links. X.25 and X.400 are examples of such transport models.

The choice depends upon the *value* of their data assets which in turn influences the *espionage risk* facing the assets. Value can be assigned differently to the same data asset by the sender, receiver or an external party not related to the sender or receiver. An external party assigning a high value to the data assets of the sender or receiver can surveil or spy at various points along the security trail, including using a cable or backbone tap of all data crossing between countries or along major transoceanic or satellite data transport paths.

People, facilities and security skills are important parts of the security trail and are directly under the control of your organization. Employees, officers and service suppliers should have compartmentalized and audited access only to data assets relevant to their immediate duties. Their backgrounds, integrity and loyalties should be investigated on a level corresponding to the value of the assets they have access to and the amount of damage they could do by abusing that access. People with poor internet and data skills are as dangerous as people who can abuse access to data assets. An organization must have very clear policies on what its computer infrastructure may be used for. Personnel must be trained to understand basic facts about e-mail, computer viruses, social networking risks and the *legal situs* location of data and transactions.

Operating systems, software and equipment may directly expose organizations to espionage or leakage of data assets when they allow "back door" access by the manufacturer or external parties or perform network transactions which are not clearly visible to or authorized by the user. This includes routers and other peripheral equipment in the data environment. The most common operating systems and software are more likely to be targeted by government and non-government parties engaged in espionage and surveillance. Many security experts currently believe that software with code that can be freely examined poses less of a risk for these dangers than proprietary software where examination of the code is restricted or not possible.

Transport protocols and routing are just as important as the other points along the security trail. The route your data assets take from sender to receiver will expose your data and transactions to various legal jurisdictions. The protocol used may simplify or prevent access by an adversary to the data in transit.

THE GIFT OF INNATE LAZINESS AND ONLINE EXHIBITIONISM

EXPERTS at national spy agencies know that government agencies, hospitals, universities, corporations, banks, hotels and airlines send billions of un-encrypted e-mails and attachments each year. E-mail is like a postcard sent through the mail. When un-encrypted, anyone can read the contents and the attachments along the data transit route. E-mails can be intercepted by recipient, sender, keyword, server or other attributes which are found in the headers. Even encrypted e-mail includes this basic un-encrypted information.

Most organizations are guilty to some degree of failing to adequately protect their data assets and private information through measures such as strong encryption of e-mail. Encryption must be effective throughout the security trail from software and operating system to transport, reception and decoding at the destination. If the information is encrypted locally but sent through an un-encrypted data transit connection, then the entire exercise is basically pointless. All points of the security trail must be covered by your security policy. One of the most common reasons for sending un-encrypted e-mails and broadcasts is that either the sender or the recipient has not implemented, does not know how to use, or is simply neglecting to utilize their existing encryption tools.

Many organizations quickly give up when confronted by this challenge because it is the path of least resistance. Spy agencies- both governmental and corporate- are fully aware of this fact. This innate laziness is perhaps the largest factor rendering e-mail interception and analysis productive and worth the efforts of espionage and surveillance projects.

An organization must also determine how much (if any) of its data assets need to be placed online to serve its clients and stakeholders. The current predominantly North American culture of "open access" should not serve as a serious guide for organizations facing a risk for espionage and misuse of the data assets they make available online. Data offered online (even with restricted access) can and usually do quickly end up on other servers in other countries and jurisdictions around the world.

All users of the data *do not* have good intentions. Think of each set or release of information your organization does online as pieces in a jigsaw puzzle. What picture or information can a spy agency or rival gain from *all* of the releases or sets of information? Neglecting strong encryption and posting potentially sensitive data assets online for eventual worldwide consumption is a literal gift from the organization to spy agencies and competitors engaged in industrial espionage.

GUIDANCE...

- Implement and consistently apply strong encryption locally and between the sending and receiving facility
- Make a policy and habit of attaching electronic signatures to official e-mails and ask partners to attach theirs. It offers an opportunity for strong encryption from the very start of the e-mail chain.
- Ensure that partners and contacts are aware of the need for strong encryption on their end and are willing to use it
- If partners will not employ strong encryption, insist that valuable data be sent by encrypted fax, telex, regular mail or via courier with a memory stick
- Never carry un-encrypted or encrypted corporate data on any media through immigration and customs of a surveillance state such as the United States, the United Kingdom, Canada, Australia or New Zealand (the Five Eyes countries)
- Do not fall for the "open access" hype! Only post data assets online which clients and stakeholders have asked for or have a legal right to access online.
- Do not post data online (with or without restrictions) which you do not wish to eventually appear in foreign and even rival jurisdictions. Even IP access restrictions will simply delay the inevitable.
- Consider regular access auditing and digital fingerprinting of the data you do make available online

GEOGRAPHY, LANGUAGE AND LAW ARE EVERYTHING

CURRENT folklore and ideology surrounding the Internet would have it that this means of information exchange is somehow stateless, exceptional and should not be restricted in any way by geography, language barriers or the rule of law. Many governments- some of them highly oppressive- would hold otherwise and want the Internet either regulated just as any other area of national communications infrastructure or divided up along the lines of individual nation states. For the sake of deliberations on corporate and agency data security, we view a middle approach as the most intelligent way of perceiving the Internet.

The fact is that the various and sundry machines, cable infrastructure and hubs that together comprise the Internet are situated in and flow through individual sovereign nations with cultures, languages and laws which are applicable also to the infrastructure and to the information which flows through it. Even if the flow of your organization's data assets takes place via a network that doesn't stop at your national borders, geography, language and law can and do act as partial protectors and potential means to maintain control of your data.

For the moment, network traffic following packet protocol is not routed in accordance with anti-spy and risk mitigation principles. The data takes the best available route at the time from a purely technical viewpoint. Most organizations ignore this fact and this can be a significant risk factor when it comes to espionage and foreign surveillance. While controlling the routing of your data assets is very difficult, it is not completely impossible with telecommunications company and internet service provider cooperation. This is especially relevant when an organization or agency needs to *avoid* data passing through a particularly undesirable legal, technical or political jurisdiction. VPN or virtual private networks as well as OSI (open systems integration) links can be created directly between the originating organization and either the destination or a trusted hub from which the data do not risk ending up in the jurisdiction or network of concern.

The possibility of alternate routing will depend upon the country you are working from and the nature of the land-based infrastructure there. In particularly difficult situations where data simply must pass through one or more known surveillance states, mobile options must be considered including satellite relay. These options are often costly, but equally effective.

Organizations should regularly check the major routes through which their data assets often pass and analyze these from a legal jurisdictional viewpoint. What are the privacy, surveillance, intellectual property protection and censorship/criminal laws in each of the jurisdictions? Servers containing valuable data assets should be located only in jurisdictions outside of surveillance states and in jurisdictions with adequate legal protections. Routing should optimally be through jurisdictions which have strong privacy protection and where adequate espionage counter-measures are taken by governments to protect communications infrastructure.

ROUTE CHECK MSK - HEL

1 185.26.112.2 (185.26.112.2) 1.210 ms 1.169 ms 1.155 ms
2 msk-m9-mr1.ripn.net (193.232.226.157) 92.859 ms 92.848 ms 92.834 ms
3 193.232.226.17 (193.232.226.17) 2.692 ms 2.654 ms 1.634 ms
4 194.186.205.149 (194.186.205.149) 42.606 ms 42.587 ms 41.480 ms
5 mx01.stockholm.gldn.net (79.104.225.38) 42.562 ms mx01.stockholm.gldn.net (79.104.225.6) 41.122 ms 41.096 ms
6 xe-5-3-2.bar1.stockholm1.level3.net (213.242.69.53) 41.317 ms
xe-8-0-1.bar1.stockholm1.level3.net (213.242.69.33) 43.521 ms
xe-8-2-1.bar1.stockholm1.level3.net (213.242.69.49) 43.478 ms
7 ae-9-2.bar1.helsinki1.level3.net (4.69.202.138) 101.113 ms 101.010 ms 100.996 ms
8 ae-9-2.bar1.helsinki1.level3.net (4.69.202.138) 100.984 ms 100.969 ms 100.950 ms
9 212.73.248.34 (212.73.248.34) 101.326 ms 101.308 ms 101.295 ms

An example corporate route check for traffic between two servers. The section marked in red indicates a hop or link in the route which causes sensitive corporate data to pass through a known surveillance state (SIGINT - Fourteen Eyes) - Sweden.

Language has also traditionally been a means to compartmentalize communication and filter information. Is it imperative that your data assets be made available in transnational languages such as English, Spanish or French? Unless your client and stakeholder groups warrant producing information in larger languages, your organization may have a great deal of flexibility in controlling the language of its data resources. Although there are currently many surveillance-state-based translators online, careful analysis of the internet protocol addresses accessing your services may allow your organization to block those services from translating your web sites or web services. Copy-protecting text on your organization's web sites may also make it impractical to translate and transfer that information to other web sites.

It is important to note that blocking automated traffic from surveillance states and known espionage centres should be done at the main server level (IP filter or Denied Hosts). The lists of internet protocol (IP) addresses to block can quickly expand to hundreds of thousands of lines. Such a large number of addresses becomes impractical for a web server to check through before allowing a regular internet visitor access and can even overload a web server.

For restricted corporate servers and hubs the situation is the inverse, requiring a limited list of *permitted* IP addresses.

Finally, organizations should clearly mark their data assets in a way that identifies the legal *situs* and regime governing the server and data. When precautions have been taken to maintain servers in specific jurisdictions and route data through specified jurisdictions (including reasonable attempts to avoid certain countries) statements of legal jurisdiction and regime will make it more difficult for spy agencies and other surveillance bodies to avoid responsibility for espionage or to claim jurisdiction when attempting to enforce foreign legislation.

GUIDANCE...

- The infrastructure of the Internet is physical and located in various legal, cultural and political jurisdictions- always base security policy on this fact
- Corporate servers and information resources should be located outside of surveillance states or states from which data assets could be made available to their espionage programs
- The corporate security trail should include policy for routing data through jurisdictions with suitable legal and technical regimes and for avoiding known surveillance jurisdictions
- Avoid the "cloud" as it very often routes data through surveillance jurisdictions or stores it in such jurisdictions
- Block automated translation services and make copying text from webpages or web services as difficult and impractical as possible
- Clearly identify the legal *situs* of servers and data

STANDARDS ARE FOR SPIES

WHEN operating systems, transport protocols, programming languages, equipment, encryption algorithms and file systems follow a similar logic or certain rules in order to get them to work together regardless of where in the world they were created it is usually the result of some technical standard. Standards aim to ensure a certain quality of performance and safety. They also serve to establish basic rules so that different equipment manufacturers, programers and end users can make assumptions about them and so that equipment, protocols and programs can properly function together. They save time for everyone involved, since manufacturers, programers and users do not have to spend time figuring out how every program, machine or connection is supposed to work. Once one is familiar with the standard, one can follow the technical assumptions of that standard and continue working with specific technical challenges not related to the basic standard or protocol.

Much like language, standards can be used to promote compatibility and communication on a global basis. Like language, they can also be used to filter communication or to limit access to your organization's servers and technical infrastructure. Two organizations using a rare, domestically-developed operating system, software developed in-house and an offshoot of an unusual standard for transport protocol for privileged server operations and communication between themselves will be relatively protected against generic attempts to surveil or spy on their operations. On the other hand organizations using all of the most usual and latest operating systems, software and communication protocols (in particular those developed and maintained in known surveillance states) are saving surveillance and espionage operations directed against their organizations huge amounts of time and expense.

The most relevant standards and protocols for deliberations on internet and data security will be TCP (transmission control protocol), UDP (user datagram protocol), SCTP (stream control transmission protocol), SMTP (simple mail transfer protocol), IMAP (internet mail access protocol), POP (post office protocol), IPv4 (internet protocol v. 4), IPv6 (internet protocol v. 6), SNMP (simple network management protocol). In addition standards for programming languages will be very relevant. Organizations must keep asking whether there are domestic or regional alternatives to these standards.

A move by your organization or group of organizations away from global and established standards or toward their lesser-known alternatives will in many cases involve a trade-off: connectivity/compatibility vs security/autonomy. The nature of an agency's or an organization's activities, data assets and clients will determine the acceptability of a particular trade-off in this area.

TRADE-OFF BETWEEN CONNECTIVITY AND SECURITY

A similar trade-off will exist in terms of expense involved in acquiring and maintaining highly secure and autonomous systems which significantly deviate from globally common standards.

GUIDANCE...

- Always deliberate on the trade-off between global, inexpensive, easy-to-find standards and security or autonomy of your sensitive data infrastructure
- Consider choosing domestic or regionally-developed equipment, operating systems and protocols if they meet your needs
- Lesser-known operating systems and standards may assist in identifying unauthorized access when spy agencies must make mistakes to understand the system
- Consider creating/using non-English-based code

BIG IS BIG BROTHER

TWO of the most notorious causes of leakage of private and protected data from the European Union and other strong privacy regions are intra-company data leakage and covert referrals. Most of the data leaked will end up stored in surveillance states such as the United States and the United Kingdom.

Intra-company leakage occurs when data collected by a branch or subsidiary of a multinational corporation ends up in another branch, division or subsidiary in a jurisdiction to which the subject if informed would not have opted to submit the information. It may occur due to logistics, an interdepartmental query or by mistake. Very large corporations or agencies will have an added tendency toward intra-company data leakage. This can pose a serious risk for your organization if you are sending sensitive queries to multinational corporations based or substantially based in surveillance states. While the multinational corporation in question may not willfully expose your data to an added surveillance and espionage risk, it may not transfer the information securely or it may itself currently be the subject of surveillance in its own state. Also, the legislation of the surveillance state in which it is based may require it to release your corporate data in a way which would be illegal where the information originated.

A covert referral occurs when contact is made from your data network by a service or someone in your organization to a specific service (usually a web page or web service) and another service or group of services (often in a surveillance state) is contacted in order to render some functionality. Servers at the site you did not intend to visit are alerted to your visit with information including your IP address, browser and computer characteristics. Thus, information about your data infrastructure is provided, without your organization's consent, to other organizations posing a potential security risk.

It is very common even for security-conscious corporations and agencies to add functionality to their public-facing web sites via "free" code snippets which in fact perform covert referrals when the web page is loaded. We consider this to be *very bad practice* when a web site is directed to organizations and agencies needing to maintain a high level of internet and data security. Organizations should utilize their own statistical applications for analyzing site usage and those applications should be based outside of surveillance jurisdictions.

There is no such thing as a free lunch, even on the Internet. Large corporations and surveillance-state-based network services offering "free" functionality tools, communications services, statistical services and data storage most often do not have a completely selfless reason for doing so. While the apparent motive may be normal corporate interests such as exposure and profit, the information gleaned from these services by the organizations offering them provides valuable raw data for corporate espionage as well as government and non-government surveillance. Organizations wholly or partly located in surveillance states, subject to the laws of those states and offering these services may have little or no option but to disclose the data to their governments. Organizations known for handling and housing very large amounts of data and international data asset traffic will be of natural interest to spy agencies.

It is easier and less expensive for your organization to go with the flow and use foreign-based free services offering "extra functionality". If you can avoid this, do so! Spy agencies and government surveillance operations are fully aware of the so-called "free-rider tendency" which tempts even government and corporate organizations which should know better to take the easy route and use ready-made applications on the Internet located on servers in surveillance states. If the potential for sensitive data leakage is low and your organization absolutely requires a certain added functionality which cannot be produced in-house, at least attempt to link to a service with *all servers* located in a strong privacy and anti-espionage jurisdiction. It's not just about your data; its about the privacy and data security of those who visit your web sites and use your web-based services.

GUIDANCE...

- Don't refer your web or web service traffic covertly to servers based in known surveillance states
- If web services that your organization needs are making covert referrals of your information when you visit them, block the IP ranges of the irrelevant servers at the router level or consider using alternative web services
- Maintain your own in-house network statistical services and added functionality tools with good privacy built in
- Ensure that your corporate internet service provider maintains servers completely outside of surveillance states and that they are fully subject to local jurisdiction

DON'T BE MAPPED

MOST employees and many employers would cringe in horror at the following sound advice: Company policy should forbid officers and employees from using the corporate network for all but essential personal activities and all entertainment, media and social networking services should be blocked by default. Few and far between are the government agencies and businesses that have such a policy. Even fewer are those that strictly apply it if they have it.

Organizations- even government agencies and corporations with sensitive data assets- are currently under enormous trend pressure to utilize international social networking services. Even without the social networking trend, it has long been commonplace for officers and employees of corporations and government agencies to post comments and ask for assistance from online forums. With access to the IP (internet protocol) address of the person who wrote the comment an interested party can collect and collate information regarding:

1. Which network (and organization) the comment was posted from
2. Other forum posts and activity originating from the same IP address and company network
3. Opinions held by certain employees which may or may not reflect corporate views and influence corporate reputation
4. Technical expertise or lack thereof among employees asking for advice in technical forums, including current corporate technical activity and possible weaknesses
5. Approximately how much time is being spent by employees and officers online
6. Whether employees are on static or dynamic network ip's and what the possible range is for the department or organization

This list of examples is far from exhaustive. The opportunities for surveillance and espionage-related data collection are ample already using the information mentioned in the list. Even in non-espionage-related cases, the data can be aggregated in jurisdictions lacking proper privacy legislation or in surveillance states and made available on completely unrelated “profile” web sites in those jurisdictions. An ounce of healthy paranoia is worth more than a pound of multilingual internet searching, lawyers and legal threats to get the aggregated information removed from each foreign site.

Even when relatively quickly removed, the information will in all likelihood already have been picked up and stored by the various spy agency robots that constantly scan the Internet moving tirelessly and efficiently along the entire global IP range. It goes without saying that such spiders or robots do not tend to respect the rules in a `robots.txt` file.

Most organizations and government agencies fail to realize that despite having two sets of corporate computers (internal computers and servers not connected to the Internet as well as those computers and servers that are connected), there is still a potential **bridge** between the two: the humans using both sets of equipment. Data assets and potentially compromising information can make their way over the "bridge" to the outside world through social networking services and discussion forums.

Many private social networking service users feel that they have more to win and little or nothing to hide when using the services. In fact, their visible network of colleagues and friends is often a source of pride. Businesses and agencies with trade secrets, client privacy agreements and valuable data assets have a lot to hide. Information about their connections, ongoing projects, future plans and the networks of their key employees and officers are prime "real estate" in the world of industrial espionage and foreign government surveillance. This has always been the case.

A visit to STASI or KGB archives and a quick look at a typical surveillance file will in many cases give a typical social networking service user a distinct feeling of *déjà vu*. Figuring prominently among the major documents in the dossier will be a schematic showing the personal connections of the subject. Everyone from family and friends to business connections and work colleagues will have their place in that schematic. It is not uncommon to see one or more adversaries noted. Sometimes even pictures and mug-shots are included with basic biographical details.

The idea behind this mapping has been: if you can't get enough information from the subject, you can from one or more of the nearest connections. And if you want to get someone close to the subject, the way to the subject is through their connections with an "introduction". This is by no means an automatic indication that any social networking service has as its prime objective to surveil or spy on its users. Many services will make attempts to protect the information of their users, both corporate and private. But the network mappings created by the users of the service themselves are an extremely valuable data asset and of definite interest to corporate espionage and surveillance.

In many strong privacy countries the creation of a database containing even basic biographical data on living persons is illegal or subject to strict regulation and restrictions on data transfer. Maintaining a mega-database of the employees and officers of strategic corporations and agencies of various countries, including their network of associates is a Pandora's box for both personal data protection and corporate espionage risk management. The information has in effect also been transferred beyond the limits of its original jurisdiction to another jurisdiction where privacy may be minimal and surveillance may be the norm.

Every corporation and agency must take a stance on the issues presented above. Are key employees forbidden from registering with any social networking site where they or their place of employment can be identified? Are they allowed to transfer their private and corporate information to a foreign jurisdiction through that registration and participation? How could the network mappings of your officers and employees be used? How extensive might the resulting damage be if the information were misused?

When considering whether to connect or disconnect from the social web, organizations and their constituents need to frankly and realistically analyse what, if any, concrete benefit they have had or most likely can have from services that map their activities and information. They also need to be aware of where the data will be stored and whether that jurisdiction allows for adequate protection or whether privacy is legally limited and the data will be located in or transferred to a surveillance state.

GUIDANCE...

- Formulate and strictly apply an organizational policy on employee or officer access to and use of any online services, especially those which can be used to map the people and activities of your organization
- Be fully informed of the server location and data transfer practices of these services and whether they are located in poor privacy or surveillance jurisdictions
- Maintain equipment and networks which are not connected to the Internet and keep them separate from servers and computers connected to the outside world allowing restricted use by officers and employees
- At the router level, block servers that violate the policy

X.400 IS BETTER THAN E-MAIL

If the OSI-based X.400 electronic messaging model were not safer, more reliable and more secure than SMTP-based internet e-mail, the intelligence community itself would not be giving it preference. The same can be said in the case of the aerospace and defence communities. The global preference for e-mail is simply a matter of cost (basically free) and relative simplicity. An e-mail system will talk to anyone- friend or foe- by design, unless there is an IP ban or blacklist hit.

Established in 1984 as a set of recommendations by the **ITU Telecommunication Standardization Sector** the X.400 messaging standards was slated to be what SMTP-based e-mail is today. SMTP-based internet e-mail "won"- at least among consumers and organizations not willing to finance or technologically adept enough to set up and maintain a decent X.400 messaging network. X.400 has a longer history of security implementations and a different link-up philosophy when compared to standard SMTP e-mail. There is not only one implementation of X.400 messaging. The defence sector has adapted X.400 to its own uses and commercial organizations have long been using versions of this messaging system compatible with their own existing EDI (Electronic Data Interchange) systems.

X.400 messages are transferred in binary format and with strong encryption between servers where the system administrators have previously vetted each other and granted each other's data traffic access. The principle of "know your neighbour" (or at least the source of your traffic) is built-in. All senders and recipients are known and valid users on vetted and approved servers. Some servers have so many vetted connections that they become hubs in the X.400 network (large, national telecommunications companies used to fulfill this role in the 1980's and 1990's). Anonymous, unknown connections are not permitted. As a member of the legitimate network, you are either in or you're out of the loop. One can in principle have a policy of only allowing servers located on national territory (or within a political region such as the EU) to become part of the network, perhaps with "guardian" servers allowing some international traffic from servers they trust.

Addressing, while not as "pretty" to some internet users as regular e-mail, takes the form:

C=country, ADMD=telecom or blank, PMDM=domain, O=org., S=surname,G=given name

Used together with very strong encryption, this messaging model has worked with TCP (same protocol used by internet e-mail) and OSI which allows for direct server-to-server or organization-to-organization connections. Virtual private networks (VPN's) can also be used in connection with the service. The X.400 messaging standard can also be used as a concurrent alternative to e-mail within the same organization- serious work e-mail versus free-for-all e-mail. Many employees and partners don't even regularly read their e-mails. Most everyone reads their X.400!

There is ample opportunity and a pressing need for non-surveillance nations to investigate and implement alternatives to common e-mail. The logic goes back in part to the discussion on standards in that section of this guide. The vetting and authentication involved in building up the X.400 network is also a tool for maintaining control over your organization's or the country's data assets. Development of alternative encryption algorithms and methods outside of the worst surveillance states and the use of these alternatives together with alternative messaging systems such as X.400 could help lower the risk of future espionage and surveillance. Other messaging methods which depend on a server-to-server connection made through strongly encrypted VPN's and where mail is deposited and accessed from a well-guarded "drop-box" should be investigated by government agencies and organizations. Messaging systems which do not advertise key servers and where addressing is in IPv6 are also an important step forward.

GUIDANCE...

- Prefer an X.400 or similar alternative messaging system to regular internet e-mail within your organization and with key partners where possible
- Locate regular e-mail servers on external-facing, non-critical systems and isolate them from your critical systems
- Consider getting government assistance in creating a large, national consortium of trusted X.400 servers where senders and receivers as well as servers are vetted and authenticated
- Adopt messaging encryption algorithms and systems which do not have a surveillance state provenance, review the provenance of other encryption-critical equipment and software

THE BIGGER PICTURE

Hundreds of millions of news followers around the world have been shocked by the past and current exposure of massive surveillance being carried out by the United States, United Kingdom, Australia, France, Denmark, Sweden and other countries belonging to the US-led Five Eyes, Nine Eyes, Fourteen Eyes, etc. spy alliances. Innocent citizens, businesses and political leaders; not terrorists, have been the subjects of this unprecedented action on the part of states whose citizens have entrusted them with protection of their rights, including the right to privacy. The legitimate business interests, trade secrets, national interests and private matters of citizens and organizations in many other countries have also been exposed to surveillance by foreign powers.

But the lesson of what has happened is not that some countries do not respect the privacy of citizens or the sovereignty of even their supposed allies. What organizations and governments can learn from these events is that ultimately they themselves are responsible for ensuring the secrecy of their trade secrets, classified information and data assets. The belief that open access, being "connected" and "mobility" are strictly positive and free from horrendous data loss and surveillance risks is a child's dream- a reflection of the technological adolescence of our current culture. Only recently, it has finally been discovered and admitted that sensitive mobile networks have in fact been infiltrated with imposter IMSI-catchers or stingray surveillance-ware placed inside of fake mobile phone stations. This is the reality we as consultants work with constantly, even before the public becomes aware of it through various mass media publications. This is the reality that your organization is in fact dealing with when it opens up its data infrastructure and networks to the outside world or "goes mobile".

The discussions, examples and guidance of the previous sections will not solve all of your problems with surveillance and espionage. Spy agencies are resilient. But if you have not even considered each of the aspects touched upon in this guide, you are far worse off in your security policy than those who have.

To our knowledge the European Union, Russia, MERCOSUR and other regions and federations have not set about creating alternative standards, alternative encryption software hubs, regional operating systems, regional X.400 networks or even systematic anti-spy sweeps of their network and mobile infrastructure. Until they do and likely even after that, the response must start with you.