



# **Future security in the office**

**A Futurizon Report compiled for Canon**

**October 2008**

Author: Ian Pearson BSc DSc(hc) CITP FBCS FWAAS FRSA FIN FWIF

©Futurizon GmbH 2008

[info@futurizon.net](mailto:info@futurizon.net)

## EXECUTIVE SUMMARY

There will be a number of changes in the ways in which we work, how our teams will be organised, and the equipment we will need. These will all have security implications.

Firstly, as artificial intelligence continues to improve, we will see the office become more of a meeting place and less focused on desk work.

Secondly, as teams become increasingly inter-company, the boundaries between companies will blur significantly. This will mean that people will work quite often with project colleagues in different companies, whom they have only known briefly. This will mean that greater focus on security in shared machines.

Thirdly, miniaturisation is probably the biggest direct hardware threat facing IT security. As devices become tiny but powerful, it will become much easier to hide surveillance devices and engage in corporate (and personal) espionage. It will also become easier to introduce harmful software into machines. This trend is already apparent with the increasing use of high capacity memory sticks, which as we have seen recently, can hold huge quantities of potentially sensitive information. In the future, a wide range of tiny devices, even electronic jewellery, will be wirelessly connected into a range of office and personal systems, and security policy will have to cope with this abundance and variety of threats.

Fourthly, paper is still a comparatively advanced information storage and display technology, unconstrained by the usual technology barriers of operating systems and software. Although electronic paper will add video and interactive functionality in due course, our high affection for paper is likely to continue, so printers, scanners and copiers will remain part of our lives for a long time yet.

Finally, it is important to recognise that staff will still need to be able to work freely if their company is to flourish, so security needs have to be delicately balanced against the need for ease of working. Security should not intrude so heavily into working practice as to interfere excessively with productivity.

## THE OFFICE OF THE FUTURE

The future office will look quite different from today's. Long term progress in machine intelligence, particularly semantic web technology that will enable a high degree of administrative automation, will automate a good proportion of today's tasks, freeing staff time to concentrate more on human relationship issues. Progress in artificial intelligence may have a similar effect, but the timescales for truly smart machines are highly debatable. In any case, there will gradually be less focus on desk work and more need for meeting areas, so we are likely to see a drive towards more desk sharing and drop-in centres, with pleasant coffee areas close by. Computer displays will partly be substituted by video visors and active contact lenses, giving wraparound high resolution 3D display capability. Those displays that are left will fill purposes such as electronic art, virtual windows, and shared media, deriving from today's electronic white boards etc. However, although there will be undoubtedly be a lot of automation of administration, there will still be

some that requires human interaction, and people will still have to produce lots of documents, with or without machine assistance. Indeed, it is likely that we will be just as fond of paper in the future as we are today.

Some meetings will only involve face to face interaction, so are easily provided for by a simple coffee area. Other meetings may involve remote presence, so it is important to have good display, audio and remote interaction capability. 3D displays are progressing quickly and are highly likely to be used in such activity. Remote touch would also be useful. Also, visualisation is useful in most industries. 3D printers or even displays that can quickly render a concept model so that groups can discuss it and interact with it are obviously useful in many fields, and virtual environments are equally useful to interact with synthesised social interactions, urban planning and so on.

As it becomes easier to work from home, and perhaps with ongoing rises in fuel costs, people will often prefer to work away from a central office. However, not everyone is suited to working from home all the time, and some of the interaction facilities described above are too expensive to be found in the average home, so a need will arise for local teleworking centres, where people can still get out of the house and go to an office environment, but they will likely share this with employees from a wide variety of different employers.

Telework centres, shared by a large number of employees, would have considerably different equipment needs compared to homes. Instead of cheap home printers, large office scanner/printer/copy centres would be more appropriate. Large displays to facilitate meetings between remote groups would be useful, as would a variety of advanced identification/verification/validation technologies. Many work groups will comprise people who will never physically meet, so it is important to be able to confirm people's identities to make secure business transactions viable. A shared and well managed office environment is also better able to provide secure communications when needed.

The ability to print electronic circuits is already well established and is likely to grow in popularity over time. This is not only useful in electronic fabrication utilities; it has a strong place in the average future office too. For example, being able to print complex circuitry into important documents can add a strong level of security, enabling much better authentication capability. Electronic signatures can be implemented by the machine printing a document, and using pens with special inks, digital seals, or biometric authentication, even human signatures can be electronically enhanced. Obviously, if machines can print electronic signatures, other machines will need to be able to read them, so this will be an important feature of future MFPs. They will need to be able to interact with the common types of RFID chips, and to read ink technology such as quantum dots and various types of micro-circuitry capsules that can be incorporated into inks.

Printers can currently print on any firm surface (even fingernails), and in the near future, it is likely that circuitry could even be printed directly onto the skin surface. A fingerprint is fine for a certain security level, but a fingerprint enhanced by circuits (or tiny magnets) printed into the skin on the fingertip would add the potential for hundreds of digits of PIN code to the actual fingerprint. Technology such as this could make it much easier to authenticate people and transactions and secure facilities. Active skin will one day be commonplace and people's skin surface can then be considered as a useful interface between machines, as well as a data storage, algorithmic and identification platform.

## FUTURE WORK/HOME BALANCE

There is already a move away from simple financial accounting for GDP, towards measures that take more account of quality of life issues such as individual happiness levels, social wellbeing, environmental quality and so on. Coupled with changes in the nature of work due to machine intelligence, we will see evolution from the information economy into the 'care economy', with more work involving human interaction, and greater social integration of companies. This pressure on companies to be more socially responsible is already apparent in the growth of CSR departments and increasing focus on PR. This is just the first stage of a long trend.

In a 'care economy' world, with companies increasingly integrated into the local community, telework centres fill a very useful dual role. People will work alongside others from the same local community, helping bind communities together, and cross fertilising ideas naturally between companies. Additionally, many of the facilities provided for a high capability work environment would also be useful 'out of hours' for a variety of socially useful activities such as adult education, training, secure network interaction (e.g. applying for licenses or other government or banking services) and even recreation. If different clientele use the buildings, it becomes even more useful to have highly capable identification and secure facilities.

The blurring of the boundaries between home and work life has already been under way for some time of course. People already deal with personal emails in the office and deal with work ones out of office hours. Companies that want staff to continue to do work on their own time, but who still try to unduly restrict social activity in the office will realise they can't have it both ways. Employees will not want to work for employers who are unduly restrictive. In any case, a dedicated employee does a great deal of their business networking and corporate PR outside of office hours. Good relations with employees are essential for this to be effective. Staff that feel trusted will respond with greater loyalty. Staff that are told to keep their social lives separate will also keep their work out of their social time, apart from complaining about it. On balance, tight security is a much smaller contributor to company success than staff commitment.

## SECURITY THREATS

In any company, workers are one of the biggest security threats, since there will always be some staff who are dishonest or open to bribery. Certainly it is already easy to record and monitor access patterns, and simple statistical analysis can spot people who routinely make certain kinds of access attempts. However, it is likely that new AI-based technology will develop that can more effectively spot inappropriate accesses. This will use other clues such as stress analysis, via posture, gesture, or direct measurement of skin temperature and conductivity. Such technology is being developed to spot potential terrorists in airports, but is equally applicable in key offices to spot people acting suspiciously.

Encryption technology is already used routinely in wireless systems, data storage and transmission. However, well publicised recent happenings with government owned data have shown that people do not always follow correct

procedures. Since people cannot always be trusted to follow guidelines, default settings on all storage and transmission technology should be that the security is enabled, and can only be disabled temporarily with correct procedure.

This will become more important as boundaries between companies and project teams are blurred. It is very hard to add security to a system once it is built, so security has to be built in at the first stages of enterprise or project creation, especially when involving collaboration between corporations. Again, if effective security is enabled by default at every layer of a system, accidental breaches can be almost eliminated and deliberate breaches much easier to track and prevent.

Staff will generally understand the need to protect key data and cooperate with essential security that is well designed and easy to work with. However, security should never become a barrier to work.

Overzealous company security policy is a potentially serious security threat in itself. Human nature drives employees to attempt to bypass procedures that get in their way when they do their job. If they want to access something forbidden by security policy, they are likely to step outside of the secured domain by using their own equipment, or by being devious. In the extremes, staff can end up doing a lot of their work on their own equipment rather than use that provided by the company. As a result, their work may be substantially outside the influence of any security that exists. A wiser policy is to work with the employees to establish a cooperative policy that they will adhere to willingly instead of trying to impose one that they are likely to be tempted to ignore or bypass.

Additionally, if a policy is too tight, but staff are nevertheless forced to follow it by some means, it might have the result of reducing performance and productivity. If it is too hard to do the job, it will take longer or not happen at all. This is obviously a threat to the wellbeing of the company, making it uncompetitive and threatening its existence. A policy designed to protect a company should clearly not threaten the ability of the company to compete by impeding the ability of staff to do their jobs well.

A more sensible security policy is one that strongly protects key intellectual property and essential systems, but is more flexible in other areas. Staff should be trusted to do their jobs responsibly, with good management and if necessary, disciplinary procedures to encourage compliance with 'common sense' and good business practice. Given greater freedom and clearly sensible boundaries, most employees respond with responsible behaviour.

However, in any company, there are hopefully rare occasions where something dubious will occur. People will succumb to temptation to cut corners, abuse staff, or otherwise engage in activity that causes someone to feel they want to tell higher management, external authorities or even the media about what is going on. The means of doing so without fear or identification are already with us.

So-called 'Onion' anonymity allows people to run blogs or access websites without being easily traceable. This kind of software was developed to allow people living under oppressive regimes to access the net or write blogs without fear of being found. It is now already being used by 'whistleblowers' to reveal information that companies would prefer to keep secret, again with a greatly reduced chance of identification.

Memory sticks are improving rapidly in capacity. Although at home, people may have large volume of music or video files that would not fit on today's memory sticks, they are able to store all the files a typical employee uses in everyday office work. Personal IT devices such as music devices and mobile phones which are commonplace today often feature wireless capabilities and can store an increasingly large quantities of data. They present an obvious direct security threat if employees use them to store confidential data, since they are easily lost, or forgotten, left in someone else's USB port. They are also a good vehicle for viruses to cross between machines, though most virus protection software protects against that. Some large companies prevent their computers from accepting memory stick connection because of this, but they are disadvantaged of course because they lose all the benefits that memory sticks bring. This is a good example of a trade-off between work flexibility and risk management. As memory sticks continue their increasing penetration into every area of everyday life, it will become necessary to have security polices that accept this use and work around it.

Ongoing IT miniaturisation is making it increasingly possible to do very sophisticated things with tiny gadgets. Putting a tiny surveillance device into an MFP, or indeed any other piece of equipment, might allow signals to be intercepted and recorded during printing or scanning tasks. Then they could sit quietly until their owner removes them for subsequent downloading. Such miniaturisation will make corporate espionage easier. In fact, as devices get smaller and smaller, there comes a time where 'smart dust' becomes so small that individual devices could be too small to be seen by the naked eye, making it almost impossible to detect devices. Since they could be largely passive, and only respond to particular types of signal, they might be hard to detect even electronically.

Personal gadgets such as social networking technology present another layer of threat. People do not stop their personal lives just because they enter an office, and in any case, a lot of work goes on outside of offices, in coffee shops and other social interaction areas. Surveillance devices can be easily concealed in everyday gadgets such as MP3 players and phones, and even the cameras built into phones now are perfectly capable of photographing documents. Since this threat has already existed for some time, it is to some extent already a known problem and dealt with by existing managerial practice. Increases in camera resolution or availability of electronic scanners just need more of the same kind of awareness.

However, every year, new devices will appear that add to the range of potential gadget-based threats. We are only a few years away from being able to incorporate almost any kind of IT function into small pieces of jewellery. A small electronic lapel pin by 2015 will likely be able to act as a personal wireless web site/blog/ego badge, that can broadcast information about that person into the nearby space and interact with badges worn by other people for social or business networking purposes. It might simultaneously act as a phone, processor, tracker, security badge, music player, video camera and perhaps many other things too. Size and shape is no constraint on function in the future. Staff will not expect to have to leave personal devices like this behind when they go to work. So companies will have to build security systems that can cope with very high levels of personal electronic functionality, with all the potential for malicious presence on those devices.

On the positive side, these technologies will obviously greatly enhance staff capability too, and in care economy roles, many of the same interpersonal functions are needed for work as for social life. So perhaps security is more at a human

level anyway, with machines doing much of the administrative work, with their own secured systems designed for machine interworking.

## SECURITY POLICIES AND TECHNOLOGIES

The future technology environment will clearly be much more complex and capable than today's, with far more directions to look for potential threats. However, the underlying human layer will be largely unchanged. Even though the social make-up will be demographically fluid, with increasing migration, ageing, and ever-changing culture, the majority of people will still be honest, good, loyal employees who present no threat except by carelessness or ignorance. Companies will have to be careful not to alienate this majority of good workers by over-zealous security policies. Trust is generally rewarded. The few who present malice will have access to extremely tiny and powerful devices, but the company will also have access to the same, so will be better able to monitor employees who are behaving suspiciously. A balanced lightweight policy that shows trust to employees and gives them the freedom to do their jobs well will be rewarded. Simple conventional security approached will continue to work well if backed up by regular education about potential threats as new technologies and new threats arrive. Staff will cooperate with policies they consider well designed and appropriate.

Also of relevance, in many countries, people are increasingly aware of governmental surveillance and the consequent loss of their civil liberty. At some point, there could well be a backlash against surveillance, and companies that are perceived to behave in this way, or to provide the surveillance technology or systems used by government are likely to find themselves in the firing line.

So the question remains how to determine when and on whom the weight of security technology should be brought to bear. Technology can certainly play a part here, via pattern recognition, gesture monitoring, stress detection, and other automated technologies largely developed for airport security. Suspicious activity and behaviour can certainly be detected automatically in many cases. However, well motivated staff who genuinely care about the company are the best defence. People are good at picking up subtle signs that colleagues may be threats to the business and can bring suspicious activity to managerial attention.

Technology developed for airport security could certainly have a good place in office security. Big companies are of course potential targets for terrorism in their own rights, so automatic detection of weapons and explosives would certainly be useful. Industrial espionage can sometimes also justify the use of behaviour monitoring or profiling too. The key issue here is balance. Some such technologies might be effective, but companies have to give much thought to the level of surveillance they want to impose on their employees, the vast majority of whom are loyal. Staff will accept surveillance at an appropriate level to the threats they perceive in their area, but will not accept high levels of unjustifiable intrusion. As always, good management is more important than the technology itself.

## HARD COPY V ELECTRONIC

One of the main reasons people print hard copies of documents is that they are easier to read than on-screen. This ergonomic problem will reduce significantly as electronic ink and electronic paper become widespread. Electronic paper can offer comparable resolution and readability to real paper, and has the advantage that it can also show video material. Electronic paper already exists, but is not widespread yet due to cost, but this will change rapidly over the next 5 to 10 years, by which time it will be very commonplace. Second generation electronic paper will allow touch sensitivity, thereby effectively becoming a full, high resolution, interactive computer display. Lying flat on a desktop, it would be much easier to read than a conventional display. Being electronic, it confers better security than paper. Biometric authentication could be required to enable the images, so that theft of the medium would not allow the thief to read the contents. However, once an image is visible, it will always be necessary to remain aware of potential onlookers. It would also be appropriate to enable electronic paper with the means to talk electronically to copiers, so that people cannot copy the information displayed on it without appropriate clearance.

Electronic paper may replace paper hard copy in many instances, but paper is unlikely to vanish. Paper is an incredibly versatile, very advanced technology, which we only look down on because it has been around for so long. If it were to be invested now, it would be considered as one of the most significant breakthroughs in the last 100 years. A medium that is cheap, versatile, flexible, lightweight, pleasant to hold, entirely future proof against all new software and hardware, which can be torn up, crumpled, heavily abused, and yet still be perfectly readable once put together again, would be considered a major advance in any other area of data storage, where files often become useless after just a couple of software upgrades. For normal everyday work where security isn't very important, copiers and printers are likely to remain important features of office life. Heavyweight security should be constrained to those areas where it is necessary.

With this kind of policy, paper printers would only be used for low security documents, and it would not be necessary to secure them at any significant level, other than the normal security associated with any office network. High security documents and data could be constrained to electronic media, and electronic paper used to extend this to purposes where the flexibility and readability of paper would normally be advantageous. Keeping secure data within a secure electronic environment with firm access procedures would make for a safe data environment for secure data, while allowing staff to work with less secure data more easily.

## COLLABORATIVE ENTERPRISES

Lines between companies are often blurred today, and this trend will accelerate, with tomorrow's business environment populated by a great many different business structures, often linking teams across large geographic distances, legal jurisdictions, and staffed by groups from different companies as well as freelancers. Improving software availability makes such flexible collaboration increasingly simple. Start-ups can get a company up and running much more easily, outsourcing key activities to off-the-shelf software, or other specialist companies. Scalability is also much easier to implement. Obviously, trust is a key issue in enabling such enterprises. Trust exists at a number of levels of

course. Where people need to use software, supplier brand is a valuable guarantor, and this brand value can be spread to third parties via recommendations. Human recruits and collaborators that are not previously known to the team need to be validated as trustworthy and competent by a trusted third party. Professional institutions are a valuable starting point for verification of professional competence, but currently are not able to verify personal trustworthiness from a security standpoint. It is likely that companies will spring up whose primary business is validation and recommendation, offering extensive security clearance services. Other technologies will develop that can use statistical and AI techniques to establish credentials of unknown people or companies. Whereas search engines such as Google return searches that only crudely sort the results, next generation search engines will offer value add by ranking according to the probable trustworthiness of the source. This will apply to data, software, companies and individual people. Of course, companies and individuals will work hard to establish their good ranking, and there will obviously be numerous attempts to corrupt the system, but the ongoing maturing of such markets will then make it ever easier to make good collaborative enterprises.

Having good staff and good software systems is then a good foundation on which to implement sensible security policies to make ongoing collaborative enterprises successful.

Such a system requires companies to work together for mutual benefit, sharing recommendation systems and knowledge about prospective candidates. The degree to which this is possible will depend on future legal systems. The UK's data protection act would currently prevent much personal data from being traded for example. However, people may find that employability depends on their own voluntary consent to such information trading. Companies may only select people from a validated pool, so prospective employees who value their confidentiality above employability might simply be excluded. In effect, subscription would eventually become effectively compulsory.

There would be some interesting spinoffs from such trust validation systems. It would for example be possible to make gadgetry that stores a person's trust profile so that it can interact with a wide range of public or corporate systems. This could evolve into an advanced identity card, automatically clearing people through immigration, authenticating them to government systems, and providing instant credit clearance or payment mechanisms. Although such systems are speculative, such an advance would also enable extra functionality for office equipment, automating a lot of the security systems described above.

As a business opportunity therefore, a well established office equipment and IT manufacturer would be ideally positioned to take a lead in such electronic validation systems. Building on a platform of improved ease of use for high levels of security, it could naturally progress via familiarity into the default platform for many other business and government services. Of course, with this future business potential in mind, such facilities should be designed with the appropriate versatility and ergonomics built in from the start, with a high level of security of course.

## LONG TERM THREATS

Technology development will continue to accelerate for the foreseeable future. As well as ongoing miniaturisation, novel threats will arise from artificial intelligence; IT/biotech convergence; advanced robotics; even from the physics of

fast networks. Robotic insects are already developing quickly, driven by military surveillance needs, but this technology will inevitably become a corporate threat too. Tiny insects might enter a building, home in on key equipment and then either spy directly, or introduce malicious software or hardware. Artificial intelligence will certainly be used to create more sophisticated virus variants, and autonomous AI entities will become threats in their own right. Today, computers act only on instruction from people, but tomorrow, they will become a lot more independent. So someone intent on mischief could create a piece of software and release it onto the net, where it could evolve and adapt and take on a life of its own, creating problems for companies while hiding using anonymity, encryption and distribution. It could be very difficult to find and destroy many such entities.

Fast networks can provide a novel means of attack. With slow networks, the time between transmissions is long compared to the physical time it takes for a signal to cross a wire to an exchange or router. As transmission speeds increase to 100s of megabits per second, the time between packets is of the same order as transmission time across the network segment. This provides an opportunity to set up resonances, especially on polling networks, such as some designs of shared fibre networks. Network resonance can greatly reduce network capacity, and if timed to coincide with high load, can throw a network into an overload situation. There are many potential variants on resonance based attacks, which can be as damaging as today's denial of service attacks. A related class of threat is the correlated traffic attack, where traffic generation can be coordinated precisely from various network points so as to generate information waves, again creating potentially overload situations. It is hard to design networks that are immune to all the types of correlated traffic types that are possible, so it only requires a reasonably expert and determined hacker to create significant network problems.

As biotech, and its advanced spinoff, synthetic biology, progress, it will eventually be possible to design and build living bacteria that can build and power electronic circuitry within their own cell. As they reproduce, large colonies of 'smart bacteria' could self organise into highly sophisticated intelligent machines, such as smart yoghurt. With this level of miniaturisation, and the ability to exist and reproduce in nature, smart bacteria could be the ultimate security threat. Bacteria floating in the air or on peoples' skin, could easily live on surfaces like keyboards, MFPs or office walls. Intercepting keystrokes as people type bypasses any electronic security that only comes into play once the information is inside the computer. Ultimately, bacteria might even be able to directly intercept brain activity, making a nonsense of any security system that involves people. In the extreme, they might even be able to control human behaviour, so really do represent an ultimate threat.

## ABOUT THE AUTHOR

Ian Pearson graduated in 1981 in Applied Mathematics and Theoretical Physics from [Queens University, Belfast](#). After four years in Shorts Missile Systems, he joined BT Laboratories as a performance analyst, and later worked in network design, computer evolution, cybernetics, and mobile systems. From 1991 until 2007, he was BT's Futurologist, tracking

and predicting new developments throughout information technology, considering both technological and social implications. He now does the same for Futurizon, a small futures institute.

He is a Chartered Fellow of the British Computer Society, the World Academy of Art and Science, the Royal Society of Arts, the Institute of Nanotechnology and the World Innovation Foundation. He also holds an Honorary Doctor of Science degree from the University of Westminster.