Secure Collaboration and the Virtual Workforce

Enabled by Microsoft® Office Enterprise 2007 Using Microsoft Office Groove® 2007

White Paper

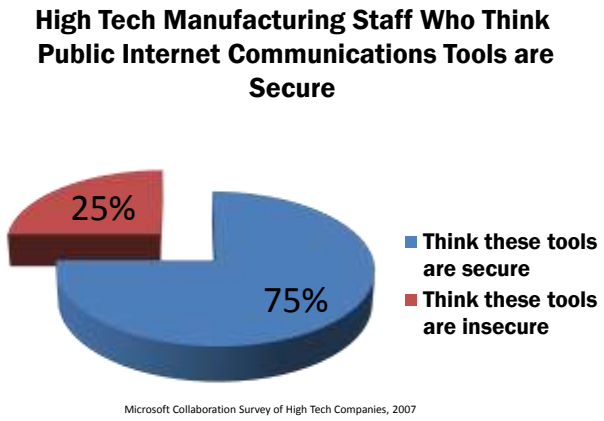
Published July 2008

Contents

Introduction

The illustrator and author, Alexander King, penned the 1960 bestseller "May This House Be Free from Tigers" referring to a sign above his front door in New York. When asked "Does it work?" he would reply, "Have you seen any tigers?"[1] Justifications for increasing security against unseen threats sometimes look like King's argument. By pointing out intangible, theoretical tigers, security experts can sound alarming. Nevertheless, there are tangible entities that seem to act like tigers in the bushes preying on information that companies would prefer to keep confidential.

Even among the most sophisticated users of technology, a 2007 research study of 200 employees in the U.S. high-tech industry found that 3 out of 4 thought that public Internet communications such as public e-mail and public instant messages were "secure."[2] At a time when people are becoming much more open in their communications through online media (such as social networking sites), commerce and governments need to exchange confidential information in a trusted manner that protects secrecy. That is particularly true of high-tech organizations, where the protection of intellectual property is of concern. As the study shows, user education is never going to be sufficient to address the need for manufacturers to keep their secrets secret.



Almost all organizations face vulnerabilities that increase the risk of damage to their reputation, their acquisitions, their revenues, their staff relations, and their equity. Finding vulnerabilities is not hard, but assessing risk by using a balanced perspective is. Organizations don't want to throw resources at paper tigers where the risks of damage are low and leave gaping holes in others where they may be acute.

The Risks

Most computer security can be summarized as keeping the bad guys from getting in and the good stuff from getting out. Most computer security focuses on the former, because the latter is deemed to be too difficult to police or requires a change in human behavior. A popular 1999 case study found fundamental usability flaws, concluding that the majority of people were not able to use Open Source encryption, PGP with e-mail. Seven years later, a similar study found that basic usability problems still remain. The challenge to maintain confidentiality is growing as more companies work in global partnerships with other organizations. Likewise, a 2007 study conducted by a major firm showed that a majority of technology company executives thought that a significant degree of their intellectual property value was being created in their emerging market business entities. A majority also said they would be increasing their partnerships and alliances in the next three to five years. As organizations become more distributed, legally and geographically, a centralized, top-down approach to security will be insufficient to protect all the "good stuff" from leaking out.

The tiger serves as a metaphor for obvious, overt threats. What if the tiger is invisible, or already inside? "We suspect that there are wide-open vulnerabilities causing valuable information to leak into the wrong places. We also suspect that many risks of covert leaks can be mitigated. Some of those risks stem from how our corporate networks are designed and built. Often, those who build and maintain the networks

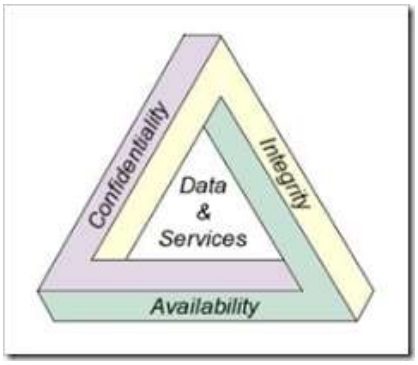
[1] "May This House Be Free from Tigers," Alexander King. 1960.
[2] "Microsoft Collaboration Survey." KRC Research. October 2007. http://download.microsoft.com/download/1/f/c/1fc50347-d273-42b0-98fb-aaa60cabf978/Microsoft%20Collaboration%20Survey%202007.ppt

become the keepers of the keys. In most organizations, digitized communications can be recorded, archived, and read by someone. Those entrusted with the keys may be outsourced, overworked staff whose skills have been commoditized. You wouldn't hand over the keys to your house to these people, but that is effectively what organizations have done with their electronic communications.

All companies distribute sensitive information among employees, to senior executives, and out to external agencies that must be secured from prying eyes. This includes financial results, M&A activity, legal documents, development plans, and compensation. Too often, these are sent via e-mail messages that may be intercepted, decrypted, stored in a fashion that is not secure – and read by unauthorized persons, putting at risk the reputation and viability of the company. All geographically distributed teams face physical and information logistics challenges staying in synch. Some members must travel great distances to meet face to face. Alternatively, if attending via teleconference, they must have in hand the information being discussed. Often, there is no common security infrastructure among separated team members – other than the public Internet and public phone networks. And if there were, it could have human vulnerabilities.

Most organizations understand the value of protecting information from unauthorized access. Internally, they can reduce that risk by encrypting data and authenticating the identities of the people using it. Most organizations erect walls around their networks and private networks to prevent external access. But this can also shut out legitimate users in other organizations with whom staff need to collaborate. With global organizational interdependencies growing, there is a greater need than ever to work securely across such firewalls. Approaches to address this interorganizational conundrum have traditionally meant a great deal of involvement by administrators. This means placing considerable trust in those people and requires a great deal of vetting and vigilance. An alternative, grassroots approach that embeds security without training is called for.

Information Security



Confidentiality, integrity, and availability are the three main elements in information security. Confidentiality should guarantee that information is only accessed by people authorized to do so, and only when there is a genuine need. Integrity ensures that stored or transmitted information cannot be tampered with. And, information should be available to authorized persons when it is needed. The need for availability, the declining cost of storage, and sheer numbers of data sources can lead to expediency at the cost of compromising confidentiality and integrity—sometimes on an enormous scale.

In October 2007, the entire United Kingdom's child benefits database——two unencrypted disks protected only by password, containing 7.25 million British families' names, addresses, dates of birth, national insurance numbers and bank account details—were sent via internal post by a junior employee at Her Majesty's Revenue & Customs to the National Audit Office. They never arrived. At the time of this writing, they have not been found. Half of the United Kingdom's adult population's confidential details are out there somewhere. It was expedient to send the disks by unregistered internal mail. It was easier and deemed to be cheaper to send the whole database rather than the specific details asked for by the National Audit Office, the intended recipient. The following month, when the loss came to light, the prime minister apologized to Parliament, the head of Revenue & Customs resigned, and the public's confidence in their government's ability to maintain confidentiality and integrity was damaged.[3]

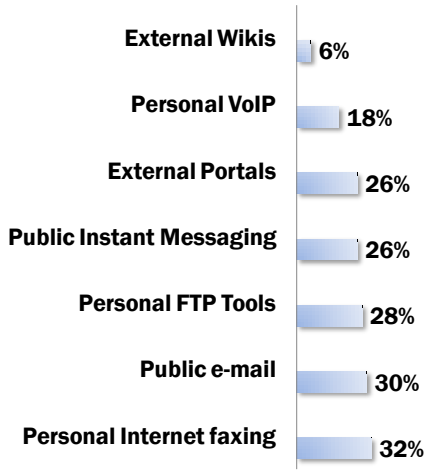
In 2007, for the third year in a row a well-known the security firm conducted a benchmark survey on data breaches. It showed a rise in the cost of data breaches in the United States, now pegged at an average of $197 per record. Lost business accounted for 65 percent of that cost. Breaches by third-party

organizations—outsourcers, contractors, consultants, and business partners—were reported by 40 percent of respondents, up from 29 percent in 2006 and 21 percent in 2005. Breaches by third parties were also more costly than breaches by the enterprise itself, averaging $231 compared to $171 per record. A common response is to implement blanket security policies and procedures. Many security policies, drafted under pressure to get things done quickly, prove to be untenable in practice. A large-scale survey[8] of IT professionals by the same firm showed that they need to circumvent their own companies' security policies from time to time. For example, to help external suppliers diagnose an IT problem, staff may be asked to transmit sensitive log files. Most people take a pragmatic view of the risk and know they need to bend the rules to keep a business running.

The 2007 survey of U.S. high-tech manufacturers unsurprisingly found that a great deal of proprietary information such as product plans and technical data were being sent as attachments over public e-mail systems.[4]

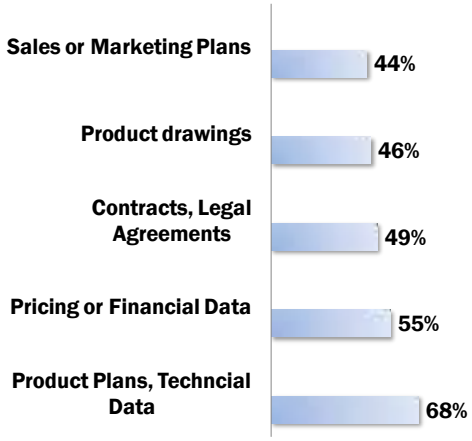
[4] "Microsoft Collaboration Survey." KRC Research. October 2007. http://download.microsoft.com/download/1/f/c/1fc50347-d273-42b0-98fb-aaa60cabf978/Microsoft%20Collaboration%20Survey%202007.ppt

Open, Public Media Used by Business Decision Makers Externally



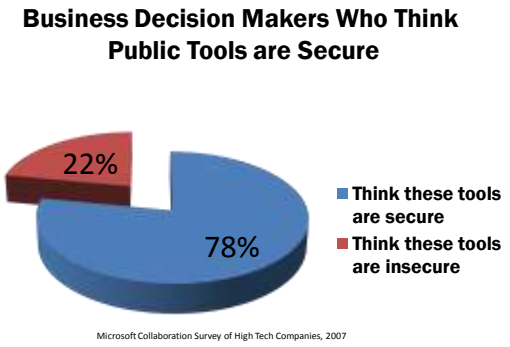
Microsoft Collaboration Survey of High Tech Companies, 2007

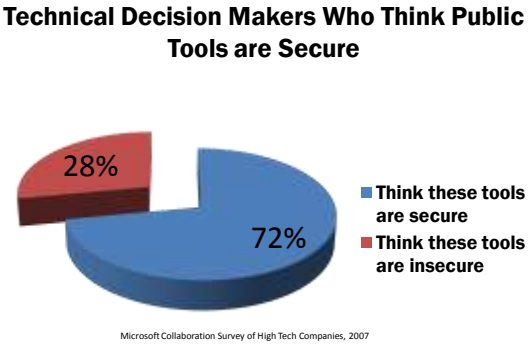
Types of Things Being Sent Over Open, Public Media



Microsoft Collaboration Survey of High Tech Companies, 2007, % of business decision maker respondents who agreed they sent these over public tools

Nearly all their companies had policies to control confidential information, and yet three-quarters of these people thought that sending this information over the public Internet was secure. They weren't your average Joe. Half were from IT departments. Many were senior executives. And they worked in high tech. If they think public e-mail is secure, what does the rest of the public think?





The truth is, most people think that public e-mail is secure. They consider it in the same category as physical mail and the telephone. With unencrypted public e-mail, there is no envelope – it is an electronic postcard that can be intercepted, and it is almost impossible to prove that a confidential e-mail message has been plucked from the ether. Perhaps those who do have an inkling that their e-mail could be purloined put their faith in security through obscurity. The safest place against mosquitoes is in a stadium full of people because the chances of being bitten are reduced by the number of people around you. But what if a mosquito has a nose only for your scent? People assume that interceptors aren't able to filter out the surrounding noise to target their specific data – and they are wrong. We are in a hurry to get digits out the door, so security is sacrificed on the altar of urgency. We do what is expedient.

Encryption

Julius Caesar took a few precautions. He used a simple encryption scheme to communicate securely with his generals, shifting letters of messages by three positions so, for example, a B would become an E. Hubris was his undoing, not hackers.
Mary, Queen of Scots, sent coded messages to her supporters who were plotting to murder Queen Elizabeth I. Unfortunately for her, they weren't up to snuff. Queen Elizabeth's secret service hacked them along with, subsequently, Mary's head. The Wehrmacht's Enigma machine took cryptography to a much more complex level. This typewriter-like device, full of rotors, was famously used to encrypt and decrypt messages during World War II. It took a huge team of people working around the clock in shifts at Bletchley Park to break the code. Their efforts may have shortened the war by two years.

For more than a decade, it has been possible to encrypt e-mail sent over the public Internet end to end, by using cryptographic techniques. But even that is no longer enough.

Because we use whatever tool is at hand, for encryption to be the norm, it has to be the default setting. It can't be a decision we have to remember to make. It is easy to say that encryption is the answer, but that leaves us with a dilemma. In the absence of a single, uniform, dominant system for verified global electronic identities, how do we safely administer the electronic keys that lock and unlock encrypted messages? Key management presents thorny issues for any large organization. Bloor Research recommends adopting a strategic approach to encryption and security by examining the balance between encrypting all traffic – with its attendant drain on system resources – and the need to get on with everyday work. Security approaches that centralize administration may depend on the integrity of a small number of individuals. If the threat from within is significant, centralization is flawed and written policies are insufficient safeguards. An approach that centralizes trust may be outdated in a world consisting of dynamic, complex, interwoven, interdependent meshes of business relationships.

Security Devolution

There is an alternate approach that devolves security to those to whom it matters most. If we want to tell a secret, we don't usually use an intermediary. We don't have centralized security in the middle. We have a direct trust relationship with the listener. We know who they are from experience. We establish a direct,

immediate, and expedient channel. It makes sense that if we are to increase security, individuals must establish their own secure channels for electronic communication, without intermediaries, with the "cone of silence" always on. That may sound daunting, but it is now possible thanks to new technology that creates self-service, virtual team workspaces for non-technical people, the most notable example being Microsoft® Office Groove® 2007.

Imagine that you had to assemble a simple team, just three people including yourself, in 10 minutes. All three of you have to be able to exchange confidential information. The other two people work in two other organizations, in different parts of the world. Neither of them is in your company's directory. Neither of them is inside your company's firewall. For security reasons, you cannot use public e-mail or public instant messaging. Getting on the phone won't get it done – you have to work on documents together. This simple example demonstrates the challenge that every team faces when it tries to form quickly across geographic and organizational boundaries and network environments. You might try to give these people a secure virtual private network (VPN) connection, but your IT department would have to be able to act very quickly and be willing to administer these types of requests on an ongoing basis.

Office Groove 2007

Microsoft® Office Groove® 2007 is guerrilla thinking for technology, as revolutionary a change to existing methods for cross-team collaboration as the PC was to the mainframe. Teams create their own enhanced security virtual team workspaces. These workspaces enable more secure, cross-firewall collaboration without other people being involved in setting up a VPN or a secured, shared Web site. This facilitates collaboration that would either not happen at all, or would be done in a manner that is not secure by using public e-mail and instant messaging.

The workspace's team leader, or delegate, grants permission to access content, consciously determining what can be done with those files, and by whom. This "roles-based" access control is an enhanced security feature that most organizations want for their own intranets and extranets, but find very difficult to implement by using a centralized approach. People keep changing hats, and many projects are short-lived and ephemeral. With self-service, virtual team workspaces, access becomes the responsibility of those who have the most knowledge of other team members, just as it is when people meet physically.

There are two basic approaches to virtual workspaces, one based on pull and the other on push. The pull model uses a self-service Web site, such as Microsoft Office SharePoint® Server 2007. This has the advantage of being highly scalable to support large teams that need open, public access to content. But people have to go get information. A common method to alert people that content has changed is to push out e-mail notifications. These can quickly become a nuisance if the information is in rapid flux. In the e-mail deluge that follows, it becomes difficult to distinguish the dross from what matters and to compartmentalize those inbox messages.

The second approach is to push content to workspaces held on local devices. Unlike Web sites, Office Groove 2007 content does not live on a server. It is based on the push approach for one reason: Virtual team content should be available offline in addition to online, but in a more secure environment. People need to travel and work on the go. That means they need to have access to a locally-stored copy of the information. You can't depend on a live browser connection everywhere, nor can you expect people to work happily on tiny devices for long stretches. To make rich drafts of content available to every team member who has a portable computer or PC, without requiring them to keep continuously connected to the Internet, local copies of files have to be kept in synch somehow. Changes made by one member need to ripple across the team to ensure everyone is looking at the latest version. Keeping complete files in synch is no simple feat. The technology must be sophisticated enough to synchronize only the changes to a document; if you synchronize the entire document every time it changes, you chew up bandwidth. If one comment is changed in a Microsoft Office PowerPoint® 2007 presentation file that each team member is meant to have, only the small data overhead of that comment must be propagated. In addition, if someone edits a document while offline, they must not inadvertently overwrite the work of someone else.

These are challenges that Office Groove 2007 has overcome, while keeping identities, messages and files more secure. Office Groove 2007 obviates public e-mail and public instant messaging, while keeping all information on projects or negotiations or events more secure and compartmentalized in workspaces.

Office Groove 2007 security features are comprehensive, yet transparent to the user. Security features are embedded, and people cannot opt out of their use. All content on local disks is encrypted, in addtion to any content sent over the network – all automatically. Should a portable computer be lost or stolen, or someone or some agency were to snoop over a network or phone connection, the security features will help keep your information safe. Multiple local copies of content created under the enhanced security features add another benefit. If Internet access goes down, locally available copies create their own resilience for the team. There is one caveat: Like teams, individual workspaces do not scale upward very well. Just as it is difficult to manage a team larger than twenty people, it becomes difficult to manage a single workspace that has more than twenty members. It is best to hive them into smaller, more manageable groups where content can be developed and shared with less confusion.

Getting Virtual Teaming Right

Virtual teams will become the norm, and preserving confidentiality and trust is only one required element for creating high-performance virtual teams. Getting distributed people to work as if they were co-located takes more than technology, though the medium plays a crucial supporting role. A recent book on the virtual workforce concludes showed that by managing “virtual distance”—the degree to which we perceive we are apart from others—organizations can significantly increase innovation behaviors, trust, job satisfaction, role and goal clarity, on-time, on-budget performance and helping behaviors.

Conclusion

Virtual team workspaces are one new way forward for dispersed teams to work. They will grow in sophistication as secure VoIP, video conferencing, and mobile phone access become increasingly part of that environment. As has been shown, you can’t mandate that people don’t use insecure channels, but you can make the secure workspace the expedient choice, as simple to initiate as an e-mail message, with richer features than e-mail, so information is organized, more accurate, fresher, and easier to find. Soon, all cross-organizational teams will be able to work as productively as if they were sitting behind one single, closed door through which no tiger would dare enter.

About the Author

Jim Moffat has worked since 1985 in the collaborative software industry and chairs the Global Groove User Group, www.grooveuser.org.