



WHITE PAPER
JUNE 2006

Employee Monitoring – Why Now?

In many senses digital communication is out of control in most organizations. This paper provides an analysis of the consequential pressing issues that drive the need for a different approach to employee communication monitoring.

Written by
David Lacey

Information Security Management Consultant
Institute for Information Security Professionals & The Jericho Forum

Version 1.0.1

Disclaimer

This White Paper is meant as a guide only. Whilst every effort has been made to maintain accuracy in all matters it is not possible to guarantee any or all of the information contained within it. No warrant is given, nor implied by the “author” - David Lacey or the “company”: Neither author or company can they be held liable for any inaccuracy or any damage or financial loss that results from any inaccuracy contained within or misinterpretation or usage of this document.

Abstract

Changes in the business, technology and security landscapes have brought the issue of employee communications to a head. Traditional management controls have broken down and many enterprise networks are now out of control as staff connect to Internet sites and freely use business facilities to exchange information with any person, any time, any where. But this situation is not acceptable. Organizations face serious security risks and tough penalties if they fail to bring employee communications under control. And traditional old-fashioned physical controls simply don't work in today's world of empowered, technology-savvy, mobile executives.

The only solution is to bite the bullet and take an entirely new approach, implementing new processes and technologies to gain better visibility and control over information flows entering and leaving the enterprise. This paper examines the relevant trends, their consequences and identifies the emerging best practices and solutions that are needed to more effectively manage and monitor the responsible use of information services by employees and contractors.

1. The New Business Environment

The communications explosion has eliminated traditional information management controls

The last two decades have seen a major transformation of the business, technology and security landscapes. An explosion of computer networking has generated a step-change in our ability to freely communicate and exchange information at any time, in any place and with whomever we like. The effect of this change has been to break down - once and for all time - the old-fashioned restrictions and hierarchical management controls of the traditional Industrial Age “cubbyhole” office bureaucracy¹ - the system that for centuries kept employees access to information in check. This transformation has opened up a Pandora’s Box of sinister new threats to business operations from worms, viruses, Trojans, hackers, spies, fraudsters and “denial-of-service” attacks. Over the last few years we have seen increasing incidents of these threats, but they are now set to move into a higher gear with the mass worldwide take-up of high-speed, always-on broadband and wireless communications, unleashing the full, latent power of the network to break down the traditional boundaries between business units, organizations and between personal and business lifestyles.

Organizations have been slow to respond to the consequences

Businesses have been slow to recognize and address the operational consequences of these unprecedented changes. But the signs of an emerging crisis are clear. Information management has collapsed in many organizations. Viruses, spam and pornography are flooding unchecked across corporate networks. Confidential information is crossing the Internet and radiating across wireless networks. Trade secrets are a hair’s breadth away from compromise. External network connectivity is out of control. And we can’t ignore or hold back this unstoppable current of change. Instead we must embrace the benefits of the free and easy communications of the Information Age and adopt radical new approaches and solutions. And we must do it now. For while our businesses have been struggling to come to terms with the challenges associated with this new networked business environment, governments and regulators across the world have already seized the initiative to create the tough new legislation and regulations that are needed to impose discipline and order on organizations.

Compliance demands cannot be ignored

Today’s management boards face a raft of legal and regulatory demands (see Section 4 of this paper for more details) forcing them to get to grips with the control of their critical and sensitive business information and the behavior of their managers and staff. And these demands apply not just within the organizations but also across extended-enterprise supply chains. The inevitable response of most organizations so far has been the typical knee-jerk one of implementing the necessary fixes quickly at whatever the cost to meet the latest legislation. And this is understandable given the novelty of the problem, the tight timescales and the severe penalties associated with non-compliance. But this approach is not sustainable. Further and tougher regulation can be expected as

¹ See Chapter 15 of Alvin Toffler’s classic book “Powershift: Knowledge, Wealth and Violence at the Edge of the 21st Century” (New York: Bantam Books, 1990) for a discussion of “cubbyholism” – the pre-computer approach of controlling and organising knowledge for wealth production.

more and more authorities recognize and address the problems, and as they broaden and deepen their demands. And, increasingly, big companies at risk will cascade tougher standards and contractual demands on their business partners and suppliers².

New solutions are needed

So how should a responsible organization respond to these increasing risks and compliance demands? Well one thing that is clear is that organizations cannot afford to simply work harder and harder to enforce traditional approaches to information management and security. Many of our existing controls won't work effectively in the new business environment. We can't transfer the controls associated with a secure office environment to an employee's home environment, an airport lounge or a Starbucks coffee shop. We can't expect to readily retrieve a key document or email from the company archives if most of the organization's information is not filed centrally but scattered across thousands of desktop computers. And we can't expect security guards to spot an employee removing large numbers of confidential documents if they can be instantly transmitted by email or downloaded onto a tiny USB dongle. In short, we need an entirely new approach.

We need new solutions that recognize that the old methods of avoiding security risks from inappropriate employee behavior - i.e. place physical barriers around sensitive information and critical processes - are no longer effective and need to be replaced by a richer, more intelligent approach that can monitor and adapt to the increasingly empowered lifestyle of contemporary business executives.

A strategic approach must be taken

On a more positive note it is encouraging to see that many smart organizations are now beginning to take a step back and assess and respond to compliance demands in a more strategic way. They have experienced the pain and expense of addressing Sarbanes Oxley or Basel II compliance requirements in a tactical, ad hoc way. They recognize that only a carefully planned, proactive approach that exploits technology, processes and people in a balanced way will enable a more efficient and effective response to the emerging risks and regulatory requirements. This paper supports that thinking and aims to reinforce that approach by assessing the key, relevant trends and their likely consequences, and by identifying the emerging best practices and the new solutions that are needed to better manage the access and use of information services by employees and contractors.

² A specific example of an Industry-driven compliance standard is the Payment Card Industry (PCI) Data Security Standard. But there is a general trend of increasing and tougher supplier relationship management across Industry.

2. Growing Pressures on Organizations

Security risks are growing

Organizations are now under unprecedented, mounting pressure to raise their game in information management, security and operational risk from all directions. The pressure is not just from regulatory compliance but also from the relentless growth in security risks to information systems, caused by increasingly sophisticated threats to vulnerable enterprise systems and infrastructures that are serving growing numbers of business users and transactions. External threats are increasing as hackers, virus writers and criminals become more sophisticated at identifying and exploiting the security vulnerabilities in IT applications and the infrastructure that underpins them. Security vulnerabilities are increasingly being exploited to attack systems well before IT service providers are able to apply corrective patches and anti-virus updates.

At the same time the potential for internal threats – whether accidental or deliberate – is growing even faster with the greater potential access capability of employees and the ease with which they can instantly introduce malicious software or remove large quantities of confidential information. These threats present a major problem for older, less secure systems that have limited capability for security improvement, having been originally designed for a more private, less hostile security environment.

The internal threat is rising

The insider threat – from accidental or deliberate action by employees, contractors or customers – has now become the greatest challenge to organizations³. Internal users today have unprecedented levels of connectivity to enterprise systems and infrastructure, and powerful tools available to download or transmit large amounts of data. Confidential information passing across networks can be intercepted from any point in the infrastructure, and malicious software can be easily introduced either accidentally or deliberately.

Organizations might suddenly find that the content of sensitive databases has been compromised by an employee planted by a criminal gang, or they may witness the instantaneous spread of a damaging virus worm across their entire infrastructure, introduced through a single external connection. And through the power of the Internet, a single embarrassing email can be rapidly cascaded to millions of external recipients, generated massive unwanted publicity and consequential reputation damage. The natural inclination of employees and contractors to be helpful, trusting and liked can be readily exploited by smart fraudsters and hackers using “social engineering” techniques⁴. And it is an impossible task to eliminate determined and sophisticated threats of this kind through policy and education alone.

³ The Association of Certified Fraud Examiners estimates the cost of employee fraud as 6% of revenue, adding up to a cost of \$660 billion in the US alone. This does not include the cost of damage from other types of security breach by employees.

⁴ “Social engineering” – a term originally coined in the 1930s in Europe to describe manipulation of engineers - is the practice of obtaining confidential information or privileged services by manipulation of legitimate users, through the telephone, Internet or email.

The costs of incidents are increasing

Many claims about security incident levels need to be taken with a pinch of salt. They are too often based on vendor spin, media spin or shallow research and analysis. And very few organizations are prepared to come clean and admit the full extent of the security breaches they have experienced⁵. But one of the few reliable independent surveys, the DTI Information Security Breaches Survey 2006⁶, indicates clearly that although security controls have generally improved across UK organizations - resulting in a leveling-off in the previously high growth in incident levels - the average cost of an incident continues to rise.

Overall, the cost of security to UK businesses is rising and is now of the order of £10 billion per year. For large businesses, that represents several million pounds each year, which is far in excess of the cost of most process improvements and new technical solutions. And the bulk of this cost is primarily the cost of business disruption, incident response and direct financial loss. Less than 10% is attributed to reputation damage - impossible to assess at the time of the incident - which is increasingly likely to impact future sales, given the steady growth in customer security awareness and concern.

Employee misuse threatens company reputation

Of more concern from the DTI Survey is the fact that web misuse dominated the worst incidents involving staff (41% involved inappropriate access and 36% excessive web surfing). Yet the Survey also reported that a quarter of UK businesses do not carry out any background checks when they recruit staff, and that 60% of them do not block staff access to inappropriate web sites. Given that top companies are likely to have brand values measured in tens of billions of dollars⁷, it is clear that organizations simply cannot afford to ignore the internal threat of employee misuse, especially at a time when traditional brands are being squeezed by media fragmentation, retailer branding and increasing consumer power. But this message may at last be getting through as the DTI Survey also reports that 90% of companies interviewed said that protecting the organization's reputation is one of the most important drivers for information security.

⁵ This situation is beginning to change with new legislation such as the Californian Law SB 1386 requiring companies to report incidents affecting the privacy of customers or employee data.

⁶ The DTI Information Security Breaches Survey is available from the PWC site at www.pwc.com.

⁷ Interbrand carry out regular surveys of brand values. The most valuable brand in 2005 was Coca Cola valued at \$67.5 billion (see www.interbrand.com).

3. The Impact of Future Trends

Market trends will fuel the growth in risks

Tomorrow's business environment will be even more challenging, with faster product cycles, volatile business partnerships, complex supply chains and a steady stream of new technologies introducing fresh sources of risk. Long-lasting and powerful trends in the marketplace will reinforce these trends. **Consumerization**⁸ of technology will result in a proliferation of new types of client device designed primarily for the consumer, not the business market. Such technology is likely to have fewer corporate-style control features and in most cases will be already in the hands of users and hackers well before it is installed in corporate infrastructures. Some organizations are already struggling to manage the security consequences of sales forces who are now equipping themselves with consumer technologies such as iPods and Skype to enhance their teamwork and productivity. This pressure on security functions will intensify with increasing vendor focus on consumer markets.

In addition, analysts at Forrester Research forecast the emergence of a powerful wave of **Social Computing**⁹ triggered by pervasive citizen communications that will transfer the balance of power over consumer perception and opinion forming from organizations to individuals, making it increasingly harder for central corporate functions to impose hard policies and rules. At the same time, the relentless **convergence**¹⁰ of data and voice communications products, services and applications will substantially increase corporate risk profiles by presenting a new set of opportunities for unauthorized access and a new range of new software technologies for attackers to exploit.

The death of corporate perimeter security

These trends will drive the final nail in the coffin for the traditional corporate-perimeter security model, requiring organizations to move to a **de-perimeterized** security model¹¹, in which critical business transactions will need to be hardened to survive in more hostile network environments, protected by security controls operating at the application and data level, reinforced by real-time security monitoring and response systems. Achieving this ambitious but inevitable goal requires a radical new approach to system design that de-couples security controls from the infrastructure and embeds them in the applications or the data itself.

⁸ The growing practice of introducing new technologies into consumer markets prior to industrial markets will be the most significant trend affecting information technology (IT) during the next 10 years, according to Gartner, Inc. As a result, the majority of new technologies enterprises adopt for their information systems between 2007 and 2012 will have roots in consumer applications.

⁹ Forrester Research believe that connections brought about by cheap devices, modular content, and shared computing resources will have a profound impact on the global economy and social structure resulting in a fundamental shift in the way companies relate to customers, with individuals increasingly take cues from one another rather than from institutional sources like corporations, media outlets, religions, and political bodies.

¹⁰ As epitomised by BT's ambitious "21st Century" IP Convergence Programme, and as demonstrated by the rapid consumer and business uptake of Skype's VoIP service.

¹¹ Deperimeterisation is defined by the Jericho Forum as "The act of applying organizational and technical design changes to enable collaboration and commerce beyond the constraints of existing perimeters, through cross-organizational processes, services, security standards and assurance." See www.jerichoforum.org for further background on this important security concept.

To achieve this end, organizations must now begin to prepare the ground by identifying and hardening their critical business applications to enable them to operate securely across an uncontrolled, potentially hostile network environment. Legacy applications that cannot be made intrinsically secure will need to be safeguarded by add-on point solutions, enhanced vulnerability monitoring, and real-time intrusion prevention and content filtering. However, despite this movement of security controls away from the corporate network perimeter, there will always be a need for organizations to maintain a clearly-defined, monitored perimeter, both as a quality of service boundary and also to define the extent of the infrastructure that is the legal responsibility of the organization.

Personal and business lifestyles are merging

And it's not just our corporate network perimeters that are being eroded by this revolution in communications. The traditional boundary between personal and business lifestyles is also melting away as employees increasingly seek to conduct personal business at work and to complete their business work at home. In the past it was easy to separate these activities, for we only did business activities in work during business hours, using business equipment. That no longer applies in a world of flexible hours and mobile communications, where employees will grab the nearest tool to hand to conduct a pressing business or personal transaction. However, this uncontrolled state of affairs cannot be allowed to continue unchecked. Organizations have a responsibility for the integrity of their business systems. They cannot allow staff to use business equipment and systems for just any purpose, for this is dangerous, irresponsible and potentially illegal. At the same time they have no right to dictate or pry on the personal lifestyles of employees - unless there is a good, sound, legal reason - because that would infringe on their human rights. Decisive, clear and responsible corporate guidance is needed, backed by a new set of solutions that are more appropriate to the lifestyle of the modern business employee.

4. The Rich World of Legal and Regulatory Compliance

An explosion of new compliance requirements

The last five years have seen an explosion in new legislation and regulatory requirements relating to corporate governance and electronic communications control. Most of this has been building for decades as governments and regulatory bodies address the new challenges and the business and societal consequences of the Information Age. But the wake-up calls of 9/11 and Enron have dramatically raised both the demands and the stakes. Legislation such as **Sarbanes-Oxley** in the US, the **Combined Code** and **Companies Bill** in the UK and new European **International Accounting Standards** require affected organizations and their subsidiaries to demonstrate a high level of information transparency, accuracy and reporting.

The scope of these compliance requirements extend beyond simple financial records, encompassing web and email communications, fraud prevention and the management, maintenance and archiving of electronic data.

- In the financial sector, **Basel II** compliance dominates the compliance agenda. This regulatory initiative requires banks to maintain comprehensive historical incident data to support formal operational risk processes. **UK FSA regulations** also require organizations - amongst other things - to maintain email records of all customer transactions for a minimum of three years.
- In the Securities Industry, the **Securities and Exchange Act 1934 17a-3/4** requires organizations to preserve customer records, including emails, and be able to retrieve them at short notice. **NASD Rules 3010/3110** also impose stringent requirements of customer records retention.
- For ISPs, the new **European Data Retention Directive** requires all details of mobile and email communications to be retained for up to two years, and for access to this data to be provided on request to police and intelligence services.
- In the retail sector, the **Payment Card Industry** Data Security Standard makes tough, prescriptive security demands on retailers accepting credit-card payments to demonstrate that customer data is safe from compromise.
- Similarly, the **Health Insurance Portability and Accounting Act** imposes tough information management and security standards on US Healthcare organizations, including strict document and email retention and archiving requirements.
- Affecting all organizations is the fast-evolving and demanding range of **Privacy, Data Protection and Human Rights** legislation imposing strict standards on the handling and retention of personal information and the rights of employees and customers.

- Combined with **Interception legislation** such as the **Regulation of Investigatory Powers Act** (UK) this requires organizations to adhere to strict, formal policies for monitoring and controlling information concerning or generated by employees, including the storage and interception of staff email and web activities.

Cascading compliance will affect all organizations

Although not all of this legislation affects all organizations, the collective impact is likely to be a progressive cascading of standards and a general “raising of the bar” in the standards expected for information management and security across all countries and sectors, as governments, regulators and large organizations follow suit in adopting and imposing standards and best practices across countries, industry sectors and supply chains. An interesting phenomenon that reinforces this trend is where the demands of a single jurisdiction are effectively cascaded across a much wider area because organizations are unable to differentiate and execute the requirements at a purely local level¹².

Audits are getting tougher

Today’s compliance requirements also involve much tougher and more thorough audits of internal controls and governance processes. Sarbanes Oxley, for example, imposes much stricter controls on the independence of auditors and audit committees. To continue to meet increasing compliance demands, companies must bite the bullet and invest in efficient corporate governance processes, supported by enhanced network monitoring and information archiving capabilities that can comprehensively demonstrate that business processes and information flows are conforming to business rules and management controls.

¹² An example of this is the Californian Law SB 1386 which requires companies that own or have access to personal data on California residents to notify them if their data has (or might have been) accessed illegally. Since it is unrealistic for organizations to separate out incidents affecting a small subset of customers, this law has the effect of imposing a general reporting requirement on all companies that might have (or work for a company that has) a customer or employee in California.

5. How Organizations Must Respond

Visibility is the key

I have long preached¹³ that visibility is the cornerstone of effective information security. That's because many of the risks and events that threaten the security of our information systems are invisible¹⁴ until they strike. On top of this, all electronic content entering and leaving the organization is invisible, unless flagged, filtered and blocked or assessed by an effective security monitoring process that can deliver an understandable alert to an interested security officer. Yet despite this, few organizations have comprehensive monitoring in place and most organizations do not even block access to inappropriate sites¹⁵. Clearly, this is a situation that cannot continue, given the mounting risks and compliance requirements. Organizations must get to grips with what is actually going on inside their offices and infrastructure. It is folly to wait until a major incident breaks out before taking action, because such incidents are merely the tip of an iceberg of bad practice. Corresponding to every major incident there are likely to be hundreds of near misses that don't get reported and perhaps many thousands of individual bad practices¹⁶.

Why we need to monitor employees

As we have seen, there are many good reasons for monitoring the behavior of employees. Here are five compelling reasons.

1. The risks from the internal security threat are growing¹⁷ and are likely to continue to grow for the foreseeable future. Organizations simply cannot afford to ignore the serious and growing threats from identity theft, fraud and illegal information brokering.
2. The financial losses and reputation damage arising from fraud or inappropriate behavior are rising and will become more significant with the increasing value of intellectual assets in a primarily Digital Economy. Even a 1% reduction in brand value would represent a loss of hundreds of millions of dollars for large organizations. And with increasing dependence on e-Business sales and

¹³ For example see my article "From the CSO's Desk: To act, first you must learn to see" in SC Magazine UK, May 2005.

¹⁴ By their very nature espionage and fraud are covert, hidden activities. There are countless examples of such activities going unnoticed for many years, including the widespread, long-lasting but highly damaging activities of "Illegal Information Brokers" in the Oil and Gas Industry which went unchecked for decades until discovered by chance in the late Eighties.

¹⁵ The Department of Trade and Industry's (DTI) biennial Information Security Breaches Survey for 2006 report says 90 per cent of companies cite protection of their reputation as one of the most important security drivers, yet three-fifths do not block access to inappropriate sites. Excessive web-surfing and accessing inappropriate sites is the second-largest cause of security incidents for large UK firms.

¹⁶ Security incidents are likely to follow a similar pattern to safety incidents. Classic research by Heinrich (1936) showed that on average, corresponding to every major incident, there are 29 minor incidents and 300 near misses. It is generally accepted that behind each major incident there may be many thousands of individual bad practices.

¹⁷ Consider for example the case of more than a dozen employees working for Mphasis, Citibank's Indian call centre partner, who were arrested last year in for allegedly stealing \$350,000 from the Bank's US customers.

- services, even a relatively short outage is likely to have a significant impact on revenue, cash flow and customer loyalty.
3. There are many intrinsic security vulnerabilities in our infrastructures - through legacy system weaknesses or unpatched platforms - that can trigger a major security incident through malware introduced by an accidental or deliberate connection of a company laptop to an external network or from the attachment of an external device to a company networks by staff or contractors. And these weaknesses cannot be eradicated without a major replacement program for key applications and infrastructure.
 4. In the absence of any monitoring software there would be no adequate deterrent to compel employees to adhere to “acceptable use” policy. There would also be no formal evidence to support any related investigations and prosecutions arising from a misuse of facilities.
 5. It would be irresponsible and potentially illegal not to monitor and maintain records of transactions with customers and critical business processes, because legal and regulatory requirements demand that organizations can readily demonstrate their operational compliance with all relevant legislation, standards and corporate policies.

Operational benefits of employee monitoring and content filtering

There are also, however, substantial operational business benefits to be gained from employee monitoring and content filtering. Consider for example the substantial savings to be gained from reductions in employee time spent surfing the Internet (which can be several hours per day per employee), or from the massive reductions in network bandwidth and storage resulting from a reduction in spam or unauthorized downloading of information or software. Levels of spam and junk mail entering the organization are likely to represent more than half of all emails received¹⁸. Smart organizations can therefore realize real cost reductions, enhanced productivity and improved response times by implementing web and email monitoring and filtering technology.

The new paradigm in employee monitoring

Faced with increasing regulatory compliance and growing risks to business operations, reputation and revenue, all organizations must now aim to raise their game substantially in employee management and monitoring. However, a new approach is needed: one that recognizes that business activities are no longer defined by the hours of the day and the location of the employee. And one that accepts that employees and contractors are mobile, work flexible hours and are likely to reach for the most convenient and nearest electronic tool when they wish to communicate for either business or personal purposes. Such an approach can only be achieved with a much richer set of solutions, based on a sensible balance and blend of policy, education and technology.

¹⁸ Jupiter Research report that the average email user received 3,253 pieces of spam during 2005.

6. Best Practice Solutions in Policy, Education and Technology

Key elements of effective employee monitoring

As with most aspects of information management and security, a holistic approach is required.

- **Policy** is needed to define the rules, promote the best practices and minimize the risks associated with this new business environment.
- **Education** is needed to equip employees with the street-wise thinking needed to recognize and address potential sources of risk, to safeguard corporate information and business transactions in hostile environments.
- **Technology** is needed to enforce corporate policies, to provide visibility of employee behavior, to detect and respond to potential violations of policy, and to deliver the visibility and evidence required to demonstrate compliance with internal corporate policy and with external legal and regulatory requirements.

Acceptable use policy

An “acceptable use” policy is not just a good idea: it is a formal requirement to enforce corporate policy and meet legal and regulatory requirements. Organizations that attempt to dismiss employees for access to inappropriate material will quickly discover that they are unlikely to succeed in the absence of a clear, written, communicated corporate policy¹⁹. But what should go into an “acceptable use” policy? The following are examples of the key items that should be included in any modern policy, although each organization will naturally have its own specific compliance requirements and views on what precisely constitutes “acceptable use”.

1. A clear definition of the **purpose and scope** of the policy, including the broad categories of information to which it applies, the people (inside and outside the organization) to whom it applies, who is accountable for maintaining, communicating and monitoring compliance with the policy, as well as who is responsible for authorizing access within the terms and conditions of the policy.
2. The **general user responsibilities** for storing and safeguarding information and for protecting account identities, passwords and other credentials. This should also address the specific and growing dangers from “social engineering” by hackers and the use of Internet and public wireless networks for business communications.
3. Clear references to existing organization **codes of business conduct**, expected standards of personal behavior and disciplinary processes, including the consequences for failing to meet the acceptable use policy itself. This should include a description of what actually comprises “**reasonable personal use**” of organization facilities, such as reading news, storing personal data, sending

¹⁹ The case of *Dunn v IBM UK* for example

- personal emails, making personal travel arrangements, Internet shopping, etc. It should emphasize that personal activities must not impact significantly on business activities. And it should set out specific **types of behavior that are not allowed**, such as undertaking activities, expressing views and entering into commitments that are likely to be detrimental to the reputation or business interests of the organization, or undertaking illegal trading using organization facilities. The policy should also define the types of **web sites that must not be accessed** (e.g. those containing material of an offensive, sexual or discriminatory nature) and the categories of **information that should not be copied or transmitted**, such as copyright or confidential information.
4. There should be a description of other specific **illegal or inappropriate activities** that are not allowed (such as sending spam, junk mail or chain letters, or the unauthorized promotion of religious or political causes) or those that might put the security of the organization at risk (such as unauthorized downloading of software or export/import of cryptographic software).
 5. And finally the policy should set out the organization policy and practice on **monitoring user activity**, including why it is necessary, for what purposes the information will be used, and also who in the organization is authorized to carry out such monitoring. And of course it should spell out precisely where, how, when and to whom to report any identified or suspected violations of the policy.

Achieving process maturity

As with many repeatable organization processes, there are levels of maturity, ranging from the most basic one of simply keeping one's fingers crossed and muddling through the implementation of the latest compliance demands – at substantial corporate risk and cost – towards the more ambitious level at which the organization learns to develop and exploit streamlined, effective processes that deliver clear business benefits from lower risks, fewer incidents, higher employee productivity, reduced data storage/communications costs and low-cost compliance management.

But these higher levels of process maturity cannot be achieved overnight, for they require enterprise-wide embedding of new processes, controls and technology, supported by pervasive education and the cooperation of managers and staff across the organization. Such an investment requires a sustained, strategic plan and a compelling business case that can deliver the long term vision in discrete phases, each with clear objectives and targets.

For example, Chronicle Solutions have developed a new process maturity framework for Information Governance²⁰ that identifies five levels of achievement ranging from the lowest level of simply “muddling through” compliance requirements, to the highest, optimizing level that delivers increasing business benefits. By exploiting such frameworks, organizations can steadily raise their game in step with the best practice achievements of other leading enterprises.

²⁰ Chronicle Solutions will shortly be publishing their new process maturity framework for Information Governance.

Education

Education of employees and other users - including contractors and customers - is vital to ensure responsible behavior and timely reporting of vulnerabilities and incidents. Yet few organizations maintain effective, enterprise-wide security education processes. By effective, I mean ones that have been intelligently constructed to take account of human psychology and failings. Employees are naturally inclined to be responsible and to follow instructions - if they make sense. In practice however most corporate educational material is poorly crafted and presented, and it simply does not resonate with staff. Psychologists will tell you that the greatest motivators for achieving an effective change in behavior are the perceived consequences of actions, especially if they're personal, immediate and certain. But few examples of the educational material developed by organizations take account of these concepts. In contrast they are generally focused on potential long-term business benefits rather than immediate personal gains, and are vague on the consequences of getting it right or wrong.

Education needs to be a carefully constructed, ongoing process with a continual drip-feed of key messages and up-to-date information, rather than a one-off, annual exercise to meet compliance requirements. Organizations that get this right²¹ can expect significant falls in incident levels. But even the very best efforts in education will never eliminate the multitude of human security failings that occur every day in every organization.

The role of technology

Technology plays a vital role in compensating for the human failings and misdemeanors of employees and any other persons who may accidentally or deliberately gain access to business systems and infrastructure. Today's electronic information exchanges are invisible, and records of business transactions and other auditable events are scattered across the infrastructure on thousands of client machines and local servers in a fragmented, duplicated yet inaccessible form.

Specialist purpose monitoring technology is the only realistic way for organizations to gain visibility of events, achieve real-time detection of inappropriate activity and maintain adequate archived records of employee communications. Such requirements are essential, not only for regulatory compliance purposes, but also to support security investigations and respond to legal claims from customers or business partners.

Smart use of technology will also deliver substantial operational benefits by helping to manage down incidents, reduce the risk of outages and minimize data storage and transmission costs. Strategically placed security technology can also compensate for security shortcomings in legacy systems by providing tighter control and assurance over confidential information flows.

The state-of-the-art in technology

Technology solutions need to be easy-to-install, transparent to applications and easy enough to be operated by a non-technical administrator or security investigator. Data storage costs are also a major consideration for communications monitoring systems, as

²¹ For example the UK Royal Mail Group managed to reduce the number of laptop losses by a factor of seven, largely through educational initiatives.

daily recorded volumes of raw transactions can amount to many hundreds of Gigabytes of storage. Intelligent compression techniques are therefore essential to reduce the large-scale duplication of content that is likely to be found across enterprise networks. And at the same time, it must also be possible to readily retrieve and reconstruct complex communications exchanges.

Chronicle Solutions' netReplay®²² is a good example of the state-of-the-art in off-the-shelf technology for automated, easy-to-operate communications monitoring. It can be easily inserted into a network and it records and indexes web and email communications in a secure, efficient and compressed form. Simple-to-operate user interfaces enable the full content of web and email communications to be captured and stored in a secure fashion, and then rapidly retrieved when required to support regulatory compliance audits or security investigations.

²² See www.chroniclesolutions.com for further information on netReplay.

Summary of Conclusions

The radical changes of the last two decades have transformed the business, technology and security landscapes, and permanently changed the way organizations manage information. The power of the network has driven a coach and horses through corporate perimeter controls and traditional approaches to information management and security, leaving organizations exposed to legal and compliance risks, and opening the door to a whole new set of sinister and damaging security threats.

Today's employees are highly empowered and have unprecedented power to access and compromise systems, infrastructure and confidential data across the organization, potentially leading to serious, irrecoverable damage to the business interests of the organization. These issues cannot be ignored for they now form part of the regulatory compliance requirements for most large organizations. And if they haven't yet hit home then they shortly will, as new compliance demands have an inevitable tendency to be rapidly cascaded across jurisdictions, business sectors and supply chains. But the traditional fixes will not work in today's new business environment of empowered, street-wise, mobile employees.

New approaches are needed. New policies that recognize that employees are no longer distinguished from other citizens by the fact they operate within business premises during business hours. Employees today are free to connect at any time to any network in support of business or personal interests. Clear "acceptable use" policies supported by ongoing education campaigns are essential to steer employee behavior in the right direction. But these softer processes alone are not sufficient. They need to be reinforced by smart use of special purpose technology that can deliver real-time visibility, analysis and reporting of inappropriate web and email communications, and enable future retrieval and reconstruction of communications to support compliance audits and security investigations.

Organizations must now bite the bullet and develop a proactive enterprise program to address these requirements, based on the classic blend of controls embedded in people, process and technology.

About the Author

David Lacey is a leading international authority on Information Security Management with more than 20 years professional experience, most recently as Director of Information Security and Risk Management for the Royal Mail Group. Prior to that, he was responsible for Information Security policy and standards for the Royal Dutch/Shell Group. Before that he was Head of IT Security for the British Foreign & Commonwealth Office. David is a keen futurist and innovator, firmly believing that the best way to predict the future is to invent it. Amongst other things, David played a major role in the development of the British Standard BS7799 and the design of the associated certification schemes. He is a regular keynote speaker at international conferences and has served on numerous professional Boards concerned with Information Security and Compliance, including the APACS Security Advisory Group, the BCS Security Forum, the Jericho Forum (which he founded) and the UK National Identity Card Private Sector User Group (which he chaired). David is also a joint founder of the Institute for Information Security Professionals (IISP) and is the first Honorary Fellow of The Jericho Forum.

About Chronicle Solutions

Founded in 2001, Chronicle Solutions is a leading worldwide provider of content centric solutions and the creator of the worlds' first enterprise-class Network Content Appliance: netReplay.

The company's mission is to provide enterprises, government and law enforcement agencies with best practice risk management, governance and compliance solutions in the Americas and Europe.

The company addresses the pressing need for large organizations to be able to monitor activities within their network boundaries and protect their internal information assets. The company's flagship product, netReplay™, is the first ever enterprise-class Network Content Appliance which captures and indexes all types of user communication on a network, on a real-time basis.

The system allows authorized managers to investigate inappropriate use of IT systems, and replay communication whether using email, Instant Messenger, WebMail, Blogs or even VoIP calls. NetReplay™ can also be used as a forensic tool in the event of a serious incident, where issues can be tracked down swiftly in a way that has simply not been possible before. Benefits of NetReplay™ include significantly reduced investigation costs and minimized losses through fraud and reputational damage.

With headquarters in London (UK), where the R&D facility is also located, and sales offices in Washington (US), New York (US) and London (UK), and representations in Canada, Mexico, Germany, France, Switzerland, Austria and Russia, the company is perfectly placed to fulfil its mission.

For further information visit www.chroniclesolutions.com