Improving User Security Behaviour

3rd September 2003

Dr John Leach
John Leach Information Security Limited
📞 = (+44) (0)1264 332 477
✉️ = (+44) (0)7734 311 567
✉️ = john.leach@jlis.co.uk
IMPROVING USER SECURITY BEHAVIOUR

Many organisations suspect that their internal security threat is more pressing than their external security threat. The internal threat is predominantly the result of poor user security behaviour. Yet, despite that, Security Awareness programmes often seem more likely to put users to sleep than to improve their behaviour. This article discusses the influences that affect a user’s security behaviour and outlines how a well structured approach focused on improving behaviour could be an excellent way to take security slack out of an organisation and to achieve a high return for a modest, low-risk investment.

A. INTRODUCTION

All modern organisations have to rely upon the sensible behaviour of their staff every day and in every operational task that their staff perform. No matter how good an organisation’s security policies and standards, security documentation simply cannot spell out unambiguously how staff should act in each situation they might encounter. Organisations cannot avoid having to rely upon their staff to make sensible security decisions for each task, no matter how small, that has any security or control element to it.

Whether diligently checking a transaction before it is released, being careful what they say over the telephone to an external caller, selecting a non-trivial password, or thinking twice before opening an unexpected and out-of-context e-mail attachment, staff are continually having to make day-to-day security decisions. If just one hundredth of these decisions were made wrongly, a large organisation would be carrying a huge weight of daily security errors causing a mammoth operational overhead.

A recent study by the ISF (Information Security Culture; The Information Security Forum; November 2000) and parallel studies of safety failures in high hazard environments (referenced in the above ISF report) suggest that as many as 80% of major security failures could be the result not of poor security solutions but of poor security behaviour by staff. Hence, a well-focused security programme targeted at improving user security behaviour could significantly reduce the size of the security-related overhead.

In this article we look at six factors that have a strong influence on people’s security behaviour. We then point to the three key factors where an organisa-
tion can take clear steps to improve its staff behaviour and, thereby, significantly reduce the internal security threat and the level of security incidents experienced.

**B. THE INTERNAL SECURITY THREAT**

The Internal Security Threat is a threat area encompassing a broad range of events, incidents and attacks all connected by being caused not by external people who have no right to be using the corporate IT facilities but by the company’s own staff, its authorised IT users.

This threat area covers user errors and omissions. It also covers user negligence and deliberate acts against the company. It encompasses behaviours such as:

- A lack of security common sense\(^1\) – users doing things that all users should know better than to do, e.g. double-clicking on an odd-looking .exe file that comes in by e-mail; sharing their password with colleagues;
- Users forgetting to apply security procedures, e.g. peripatetic staff failing to take back-ups of their desktop data; support staff resetting a user’s password on the strength of an incoming telephone call;
- Users taking inappropriate risks because they did not appreciate or believe the level of risk involved, e.g. leaving the PC unattended in an open office without logging off;
- Deliberate acts of negligence, users knowingly failing to follow essential security processes, e.g. e-mailing a highly sensitive document outside the company without any protection; support staff failing to keep infrastructure patched simply because it is “too difficult”;
- Deliberate attacks, users purposefully acting against the company’s interests, perhaps because they feel angry with their employer, e.g. disclosing a clearly restricted and highly sensitive report to the competition; disclosing significant security vulnerabilities to an outside bulletin board.

Poor or unacceptable user behaviour is a significant, perhaps even the major, determinant of the level of security incidents suffered by a company. User

\(^{1}\) The OED defines *common sense* as “sound practical sense especially in everyday matters”. By extension, *security common sense* is sound practical sense in everyday security matters.
behaviour can be improved through a variety of interlocking techniques which together work to create a strong security culture and to strengthen the way the security culture influences the behaviour of individual users. As the internal threat is possibly the largest source of an organisation’s security pain, there is potentially a huge value to be gained from understanding how this could be done.

C. THE FACTORS THAT INFLUENCE SECURITY BEHAVIOUR

To manage down the internal security threat, we need to understand how a company’s culture and practices can affect people’s behaviour.

The influential factors fall into two groups, as illustrated in the diagram below. The first group, encompassing the user’s understanding of what behaviours the company expects of them, is distinct from the second group, factors which influence the user’s personal willingness to constrain their behaviour to stay within accepted and approved norms.

The user’s understanding of which behaviours are expected of them – shown in the top half of the diagram - are formed from:

- What they are told;

Fig. 1 - The Factors That Influence User Security Behaviours

The user’s Security Common Sense and decision making skills

Internal Security Threats
- User security errors;
- Security carelessness;
- Security negligence;
- Security attacks.

User Security Behaviours

The user’s Psychological Contract with their employer

The user’s personal values and standards of conduct

The behaviours demonstrated by senior management and colleagues

The user’s Security Common Sense and decision making skills

The Body of Knowledge (Values, Policies, Standards, Procedures, etc.)

The user’s understanding of what behaviours are expected of staff

The effort required for compliance, and temptations not to comply
I. WHAT EMPLOYEES ARE TOLD

Most organisations have a security manual which comprises the company’s formal statement of its position on security. This lays out the company’s security policies, practices, standards and procedures. It might include an explicit statement of the company’s security values and principles, though it is more likely that the values and principles will be articulated only implicitly through the policies and standards laid down. This documentation can be called the company’s Body of Knowledge.

The Body of Knowledge’s effectiveness at conveying what constitutes approved security behaviours varies according to:

- Its accessibility
- The completeness of its coverage;
- The clarity of the stated security values;
- The uniformity of its security values;

II. WHAT EMPLOYEES SEE IN PRACTICE AROUND THEM

Whether they are new staff trying to understand how to behave within their new company, or existing staff more subliminally conforming to the norms of their work environment, people are very strongly influenced by the behaviour of their peers. They build their security attitudes and set their own security behaviour according to:

- The values and attitudes demonstrated in the behaviour of senior management;
- The consistency between the company’s stated values and the evident behaviour of their peers and colleagues;
- Whether other of the company’s practices (e.g. its HR practices, its PR practices) reflect its security values.
- Whether the company demonstrates that good security is important through having systems to monitor security behaviour, reward good behaviour and respond to bad behaviour.

When there are numerous inconsistencies between the formal statements in the Body of Knowledge and what the person observes in practice around them, people will be guided more by what they see than by what they are told.

III. THE USER’S SECURITY COMMON SENSE AND DECISION MAKING SKILLS

The body of Knowledge cannot hope to spell out the correct security decision for every situation the user might encounter. It should, at a minimum, cover those situations where following a particular procedure correctly is crucial. It cannot grow to encompass every situation; it has to avoid becoming so extensive that the atoms of information buried within it become inaccessible to well-intentioned but fully stretched users. Hence, staff cannot avoid having to make their own security decisions as part of their daily tasks.

Staff make most of their security decisions in non-critical situations where moderate deviation from the ideal decision can be tolerated. Some decisions will be made in critical or sensitive situations where the user has to make an instant decision about what to do without any reference to written guidance. Over a period of time, each person builds up their own personal history of security decisions made. These they will remember as either good decisions or bad decisions according to the feedback, if any, they received. In the absence of criticism, a decision will be adopted as an acceptable course of action available to be repeated until a better course of action presents itself. In this way, users build their own personal and private body of knowledge to supplement the shared corporate Body of Knowledge.

These three factors combine to create the user’s understanding of the accepted and approved behavioural norms at work. We now need to look at the factors that influence the user’s personal willingness to constrain their behaviour to stay within those norms. Their willingness to conform is affected by:
- Their personal values and standards of conduct;
Their sense of obligation towards their employer;
The degree of difficulty they experience in complying with the company’s procedures.

We’ll now look at each of these in turn.

I. **THE USER’S PERSONAL VALUES AND STANDARDS OF CONDUCT**

Most employees ascribe a high value to principles and believe in the importance of shared values and sensible rules. These employees can be expected to take up and apply the company’s system of values and standards, feeling more comfortable working amongst others to an agreed set of rules than working to their own proprietary rules or with no rules.

Tensions can arise when there is conflict between the individual’s values and the company’s values. Most people will not sustain that tension for long, and will either modify their principles or leave the company. Hence, this tension is self-resolving and rarely leads to problems. There is little an organisation can do to address this situation, and we will not discuss it further here.

II. **THE USER’S SENSE OF OBLIGATION**

Employees feel a psychological pressure to behave according to company expectations, voluntarily to constrain their behaviour to stay within the bounds of accepted practice. A large part of this pressure comes from what is called the “Psychological Contract” between employee and employer. For some this pressure is stronger than for others.

Each employee has a psychological contract with their employer, an unwritten reciprocal agreement to act in each other’s interest. The employee agrees to work diligently at their job and to conform to the company’s behavioural expectations in return for the company treating them well.
It is in the nature of a contract that each party honours the contract to the degree that they perceive the other party to be honouring it. Hence, if a member of staff feels they are well treated, recognised and rewarded, they will gladly respond in kind and act in the company’s best interest. If they feel they have been treated unfairly by their employer in any area of their employment relationship, they will feel that the bonds have been loosened and will not feel as obligated to act in the company’s best interests. Indeed, if the person feels the company has done them wrong, they could feel angry and compelled to punish the company. That is when a company’s users become its security enemies and can become the source of major security threats.

Companies recognise that the rewards of work vary from individual to individual. For some people, work is largely about being in a social environment with others. For some, work is about earning a salary to pay the mortgage and buy the toys. For others, it might be about getting good training and experience as they move quickly on their way to other positions in other companies.

Whatever their reasons for working, people will feel varying degrees of satisfaction and reward from being at work. Their level of satisfaction will determine the strength of their psychological contract with their employer. The strength of their psychological contract will determine the degree to which they constrain their behaviour to conform to approved and acceptable company norms.

III. THE DIFFICULTY OF COMPLYING

The third component is whether the company makes it easy for their staff to comply with its standards and procedures, and whether there are temptations of personal gain seducing people not to comply.

If security controls are difficult to perform or are operationally burdensome, if they are of little obvious benefit or do not effectively prevent people exploiting opportunities for personal gain, users will have a natural incentive to circumvent the controls. Even when staff recognise that security controls are implemented for good reasons, they have very little tolerance for controls that are not effective, not efficient, or not clear. The knowledge that their behaviour is being monitored and their compliance measured, and the weight of any penalties used to discourage non-compliance, will have some limited effect on how far staff are prepared to let their behaviour stray from mandated norms, but they do nothing to improve staff attitudes towards security.
D. THE KEYS TO BETTER USER SECURITY BEHAVIOUR

These are the six influential factors affecting how users behave. Clearly, a company can expect to influence some but not all of these. A company cannot expect, for example, to have much influence over its staff’s personal values and standards of conduct, or their intrinsic belief in the benefit of following rules.

Companies will best manage down their internal security threat by focusing primarily on those factors that are realistically within their control. They need to get the most leverage they can out of the factors that they can influence, for they cannot presume that all staff will bring to their work high personal standards and a natural faith in the value of following rules.

Three of the above six factors are key to improving security behaviour and driving down the impact of the internal security threat. We will focus on these three, discussing them in just a moment in the sections below. The other three, lesser factors, we can deal with quickly here.

- As we have just seen, a company cannot expect to have much influence on its staff’s personal values and standards of conduct, or their intrinsic belief in the benefit of following rules. The best course of action is fairly to divert contra-indicated staff away from roles where the company is most exposed to any shortfall in the standard of its staff’s behaviour.

- The company should make continual efforts to ensure that its Body of Knowledge is readily accessible to all its staff. It should recognise that different staff will need to receive different messages and receive those messages through different channels. Building a strong Body of Knowledge is not a trivial task. However, it is well covered in the literature at large and we do not need to discuss it further here.

- The company should make continuous efforts to ensure that its security controls are efficient, effective, and properly positioned. This is a labour of continuous improvement. However, it is also obvious and we do not need to discuss it further here.

The three factors that are key to improving user security behaviours are:

- The behaviours demonstrated by senior management and colleagues;
The user’s Security Common Sense and decision making skills;
The strength of the user’s psychological contract with the company;

We shall look at each of these in turn.

I. THE BEHAVIOURS DEMONSTRATED BY OTHERS

What people see in practice around them influences their attitudes and behaviours more powerfully than what they are told. The company’s Body of Knowledge will be undermined if its stated principles, policies and procedures are contradicted by the practices that people see in evidence around them. What people are shown needs to support rather than to contradict what they are told.

If a company wants its users to practice correct security, it needs to back up this desire with systems to ensure that its principles and policies are followed. If a few bad security practices are allowed to establish themselves, all security practices are weakened in the eyes of staff. Ensure that all senior management as well as junior staff have good security behaviour. Make a point of providing feedback to staff on the correctness of their behaviour, and of gathering input from staff on where the Body of Knowledge is being undermined by contrary messages in the company’s pronouncements or contrary practices in its systems. Reward staff for good security behaviour, and require additional training or take other appropriate steps for staff that demonstrate unacceptable behaviours.

II. THE USER’S SECURITY COMMON SENSE AND DECISION MAKING SKILLS

A user’s own security decisions, once made, become a part of the user’s personal body of knowledge and carry forward into their future security decisions. Therefore, a company has a clear requirement to help its users develop good security common sense so they can make simple and straightforward security decisions reliably and correctly themselves. Otherwise it will not escape suffering a high and persistent background level of security worries, such familiar mistakes as people forgetting to change default passwords on newly installed equipment or using their own remote dial-in facilities to avoid having to use the corporate managed gateway.

Common sense is about having a realistic practical understanding of how things work in the real world and being able to make good practical decisions unguided. Deciding whether or not to believe what one hears, deciding how to
follow an unclear instruction, and making tough decisions in complex situations all require sound common sense. Common sense is something that everyone recognises when they see it. It is a decision-making skill, not simply an accumulation of knowledge.

Security common sense is something that can be taught. Teach the user the principles they need to guide their decision making, but keep the number of examples down to those few needed to illustrate the principles. Avoid providing too many examples. Too many examples and you will be taking decision making away from the user and putting it back in the Body of Knowledge. You will leave the user with weaker, not stronger, decision making skills. This is where many Security Awareness and Education courses go wrong.

Focus on developing the users’ security decision-making skills. Thereafter, provide people with continual feedback and support. Give them credit when they do something well, and let them know when they err, indicating a better decision they could have made. Periodically refresh them with widely applicable examples so that users can continually re-centre their decision making framework and prevent it wandering off centre over time.

III. **THE USER’S PSYCHOLOGICAL CONTRACT WITH THEIR EMPLOYER**

If a company ensures that its overt behaviours support rather than contradict its Body of Knowledge, and it helps staff develop and strengthen their security common sense, it will reduce the number and severity of user security errors. It will also want to reduce the willful component of the internal security threat: user security negligence and deliberate attacks by the user. That is addressed by ensuring that users feel strongly bound by their psychological contracts with the company.

We return to the observation made above that it is in the nature of a contract that people will honour their psychological contract to the degree that they perceive the company to be honouring its part of the contract. Hence, a company can bind its users to its code of good security conduct by showing that it is bound to the code itself.

Earlier in our discussion, the issue was one of ensuring that practice on the ground was not allowed to contradict the Body of Knowledge. Here the issue is to ensure that the company is boldly seen to be taking security seriously rather than timidly keeping its security efforts hidden from view. This issue is, of course, closely interwoven with the earlier issue and both aspects contribute to the creation of a strong security culture. The creation of a strong security
culture is the best way to motivate staff to behave consistently in a security-conscious way.

Look for guidance from the practices of companies with strong safety cultures. In companies working within high-hazard industries, one would expect to see safety discussed regularly by senior management, both in board and strategy meetings and in communications with staff. Safety issues would be reported on regularly and openly, and shortcomings would be treated as serious issues warranting urgent management attention. Safety mandates carry conviction, and staff are consistently safety-conscious.

For a company to strengthen its security culture, it should expect to follow similar practices. Be seen to be discussing security issues at senior management levels and make security a topic of regular communication with staff. Report on security issues openly within the company. Deal with serious shortcomings under senior management direction. Show clearly that security is an important part of how senior management runs the business. Then the corporate security mandates will carry conviction, employees will be consistently security-conscious, and staff will align their behaviour to the corporate security mandates.

The converse is too familiar. If security does not feature in discussions or communications, and the company’s senior management acts inconsistently from issue to issue, staff will perceive the company to have a weak security culture and will not consider themselves duty-bound to follow company mandates. They will not expect to do any more themselves than they see other people do, even if it falls well short of the written policies. If staff feel their corporate superiors do not demonstrate that honouring corporate values and principles is important, they will not make any effort to abide by the rules themselves other than by default.

It is a simple matter of leadership. Strong leadership creates a strong culture, and a strong culture gives clear direction to staff at all levels.

This helps illustrate why honour and strong leadership are so important in the fighting forces, where men and women might be called upon to push themselves to their limits and to put themselves in positions of personal danger. Interestingly, this also illustrates why companies with a weak corporate culture find culture change so difficult, whereas one might at first have expected that they of all companies would find culture change relatively easy.
E. CONCLUSION

A company’s primary objective in influencing its users’ security behaviour is to drive down the level and severity of the security incidents it experiences. Poor user security behaviour is a significant, perhaps even the major, determinant of the level of security incidents a company suffers. Hence, companies have a ready opportunity to make significant security gains by having a strong security culture and by strengthening the influence the culture exerts on individual users.

Of the various influential factors, we have focused on three that are key. A company can maximise its leverage from these three if it:

- Makes sure that the behaviour of senior management and the company’s systems support rather than contradict the Body of Knowledge;
- Strengthens the users’ security common sense and trains staff to develop good security decision making skills;
- Makes sure that senior management is seen to be taking security seriously and demonstrates that good security behaviour is important to the way the company operates.

Leadership is the key. After all, if senior management can’t be bothered, then why should staff?

The ways to improve User Security Behaviours

[Diagram showing the relationship between factors affecting user security behaviours, including the Body of Knowledge, the user’s understanding of expected behaviour, the user’s willingness to constrain their behaviour, the user’s personal values, internal security threats, and the effort required for compliance.]

Internal Security Threats
- User security errors;
- Security carelessness;
- Security negligence;
- Security attacks.

The user’s Security Common Sense and decision making skills

The user’s personal values and standards of conduct

The user’s Psychological Contract with their employer

The behaviours demonstrated by senior management and colleagues

The user’s understanding of what behaviours are expected of staff

The user’s willingness to constrain their behaviour to stay within accepted norms

The Body of Knowledge (Values, Policies, Standards, Procedures, etc.)

The effort required for compliance, and temptations not to comply

Leadership is the key. After all, if senior management can’t be bothered, then why should staff?