

Information Security Management



What is it?

Information is the life blood of a company regardless of the size or nature of the company and no matter where that information is stored. It could be in filing cabinets, on computer systems or in staff members' heads. It could be client details, contacts, financial records, contracts or product data. It needs to be managed and needs to be protected.

Information security protects that information from a wide range of threats in order to ensure business continuity, to minimise business damage and to maximise the return on investments and business opportunities.

There are four main characteristics of information security:

- Ø Confidentiality – making sure only the right people see the information;
- Ø Integrity – making sure the information is correct and isn't tampered with;
- Ø Availability – making sure it is available when it is needed;
- Ø Repudiation – the risk that someone else will reject the information as incorrect.

Why might you need it?

Major events like September 11th do not happen every day but less serious events do occur all too frequently and are often outside your control. Strikes by postmen, fire, flood, hackers, bombs, gas leaks, viruses, etc. can all affect the profitability and ultimately the viability of your company. Taking suitable precautions to deal with possible eventualities is what Information Security Management is all about.

Do you need it?

Ask yourself the following three questions:

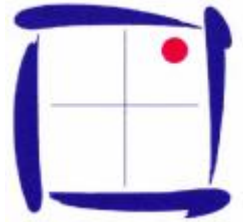
“How long could I manage without the information I currently take for granted – contact information, production data, orders, financial information, staff details, or something else equally important?”

“How long would it take me to get that information back if it was lost, it was damaged, or was unavailable for some reason?”

“How likely is it that this information could be lost, damaged, altered unintentionally or otherwise unavailable?”

If your answers are honest there is a high probability that at least some of your information could be fairly easily lost or damaged in some way or another, would take several hours if not longer to recover, and would seriously affect your business operations in the meantime. This is why information security is so important.

Information Security Management



So how do I go about it?

It is not possible to remove all risks to your information and indeed it is unlikely that you need to deal with all information in the same way. So there are a series of steps to take to address the main issues.

- 1. Undertake a risk assessment for all your information. This means for each type of information considering the business harm likely to result from a security failure. This is achieved by first reviewing the potential risks and their impact on the confidentiality, integrity, availability and repudiation of the information and other assets. Then the realistic likelihood of those risks occurring in the light of current threats and vulnerabilities.*
- 2. On the basis of this evaluation, decide which sets of information need most care and consider the alternatives available to you to look after it.*
- 3. Information of limited value, at low risk which can quickly and easily be replaced might not be safeguarded at all. For information which is of much higher value to your company, at greater risk or much more difficult to replace, you might decide to take backup copies, lock away (either electronically or physically), limit access to essential users and so on. These are called the controls and it is a management decision what sort of controls you choose, the information you choose to control and the degree of control exerted.*
- 4. The choice of controls is usually in three areas: physical (locking things away); technical (password protection, anti-virus protection, etc.) and procedural (terms of reference, company rules, segregation of duties, etc.). Not all are applicable for all types of information, for all types of company or for all types of risk and so a balanced mixture must be chosen.*

Is there any guidance available?

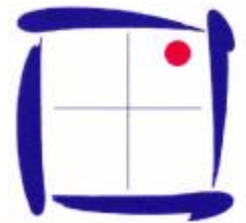
The most useful starting point is to consider the British Information Security Standard BS 7799 which was recently adopted as an international standard, ISO 17799. This standard, if properly applied, will provide for all your information security requirements. It covers ten areas to consider when reviewing your information security.

You choose which parts of the standard you apply and which bits you ignore. Naturally you would need to justify those areas you do not implement, if you choose to become ISO 17799 certified. These are management decisions, and could be based on, for example, cost, perceived lack of threat or other similar reasons.

Do I need help to do this?

Your company should be able to maintain the systems put in place without specialist help. However, it may be beneficial to have someone with whom you can discuss the issues, and provide expert advice and guidance as you implement your programme. Andy Taylor, of ValueAdding.com, can provide this for you and your organisation.

Information Security Management



What is it?

Information is the life blood of a company regardless of the size or nature of the company and no matter where that information is stored. It could be in filing cabinets, on computer systems or in staff members' heads. It could be client details, contacts, financial records, contracts or product data. It needs to be managed and needs to be protected.

Information security protects that information from a wide range of threats in order to ensure business continuity, to minimise business damage and to maximise the return on investments and business opportunities.

There are four main characteristics of information security:

- Ø Confidentiality – making sure only the right people see the information;
- Ø Integrity – making sure the information is correct and isn't tampered with;
- Ø Availability – making sure it is available when it is needed;
- Ø Repudiation – the risk that someone else will reject the information as incorrect.

Why might you need it?

Major events like September 11th do not happen every day but less serious events do occur all too frequently and are often outside your control. Strikes by postmen, fire, flood, hackers, bombs, gas leaks, viruses, etc. can all affect the profitability and ultimately the viability of your company. Taking suitable precautions to deal with possible eventualities is what Information Security Management is all about.

Do you need it?

Ask yourself the following three questions:

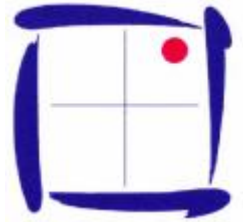
“How long could I manage without the information I currently take for granted – contact information, production data, orders, financial information, staff details, or something else equally important?”

“How long would it take me to get that information back if it was lost, it was damaged, or was unavailable for some reason?”

“How likely is it that this information could be lost, damaged, altered unintentionally or otherwise unavailable?”

If your answers are honest there is a high probability that at least some of your information could be fairly easily lost or damaged in some way or another, would take several hours if not longer to recover, and would seriously affect your business operations in the meantime. This is why information security is so important.

Information Security Management



So how do I go about it?

It is not possible to remove all risks to your information and indeed it is unlikely that you need to deal with all information in the same way. So there are a series of steps to take to address the main issues.

- 1. Undertake a risk assessment for all your information. This means for each type of information considering the business harm likely to result from a security failure. This is achieved by first reviewing the potential risks and their impact on the confidentiality, integrity, availability and repudiation of the information and other assets. Then the realistic likelihood of those risks occurring in the light of current threats and vulnerabilities.*
- 2. On the basis of this evaluation, decide which sets of information need most care and consider the alternatives available to you to look after it.*
- 3. Information of limited value, at low risk which can quickly and easily be replaced might not be safeguarded at all. For information which is of much higher value to your company, at greater risk or much more difficult to replace, you might decide to take backup copies, lock away (either electronically or physically), limit access to essential users and so on. These are called the controls and it is a management decision what sort of controls you choose, the information you choose to control and the degree of control exerted.*
- 4. The choice of controls is usually in three areas: physical (locking things away); technical (password protection, anti-virus protection, etc.) and procedural (terms of reference, company rules, segregation of duties, etc.). Not all are applicable for all types of information, for all types of company or for all types of risk and so a balanced mixture must be chosen.*

Is there any guidance available?

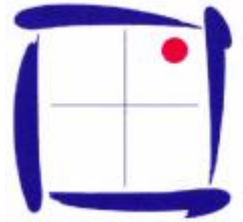
The most useful starting point is to consider the British Information Security Standard BS 7799 which was recently adopted as an international standard, ISO 17799. This standard, if properly applied, will provide for all your information security requirements. It covers ten areas to consider when reviewing your information security.

You choose which parts of the standard you apply and which bits you ignore. Naturally you would need to justify those areas you do not implement, if you choose to become ISO 17799 certified. These are management decisions, and could be based on, for example, cost, perceived lack of threat or other similar reasons.

Do I need help to do this?

Your company should be able to maintain the systems put in place without specialist help. However, it may be beneficial to have someone with whom you can discuss the issues, and provide expert advice and guidance as you implement your programme. Andy Taylor, of ValueAdding.com, can provide this for you and your organisation.

Information Security Management



What is it?

Information is the life blood of a company regardless of the size or nature of the company and no matter where that information is stored. It could be in filing cabinets, on computer systems or in staff members' heads. It could be client details, contacts, financial records, contracts or product data. It needs to be managed and needs to be protected.

Information security protects that information from a wide range of threats in order to ensure business continuity, to minimise business damage and to maximise the return on investments and business opportunities.

There are four main characteristics of information security:

- Ø Confidentiality – making sure only the right people see the information;
- Ø Integrity – making sure the information is correct and isn't tampered with;
- Ø Availability – making sure it is available when it is needed;
- Ø Repudiation – the risk that someone else will reject the information as incorrect.

Why might you need it?

Major events like September 11th do not happen every day but less serious events do occur all too frequently and are often outside your control. Strikes by postmen, fire, flood, hackers, bombs, gas leaks, viruses, etc. can all affect the profitability and ultimately the viability of your company. Taking suitable precautions to deal with possible eventualities is what Information Security Management is all about.

Do you need it?

Ask yourself the following three questions:

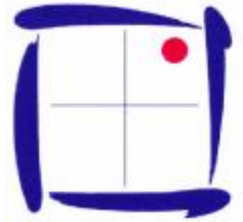
“How long could I manage without the information I currently take for granted – contact information, production data, orders, financial information, staff details, or something else equally important?”

“How long would it take me to get that information back if it was lost, it was damaged, or was unavailable for some reason?”

“How likely is it that this information could be lost, damaged, altered unintentionally or otherwise unavailable?”

If your answers are honest there is a high probability that at least some of your information could be fairly easily lost or damaged in some way or another, would take several hours if not longer to recover, and would seriously affect your business operations in the meantime. This is why information security is so important.

Information Security Management



So how do I go about it?

It is not possible to remove all risks to your information and indeed it is unlikely that you need to deal with all information in the same way. So there are a series of steps to take to address the main issues.

- 1. Undertake a risk assessment for all your information. This means for each type of information considering the business harm likely to result from a security failure. This is achieved by first reviewing the potential risks and their impact on the confidentiality, integrity, availability and repudiation of the information and other assets. Then the realistic likelihood of those risks occurring in the light of current threats and vulnerabilities.*
- 2. On the basis of this evaluation, decide which sets of information need most care and consider the alternatives available to you to look after it.*
- 3. Information of limited value, at low risk which can quickly and easily be replaced might not be safeguarded at all. For information which is of much higher value to your company, at greater risk or much more difficult to replace, you might decide to take backup copies, lock away (either electronically or physically), limit access to essential users and so on. These are called the controls and it is a management decision what sort of controls you choose, the information you choose to control and the degree of control exerted.*
- 4. The choice of controls is usually in three areas: physical (locking things away); technical (password protection, anti-virus protection, etc.) and procedural (terms of reference, company rules, segregation of duties, etc.). Not all are applicable for all types of information, for all types of company or for all types of risk and so a balanced mixture must be chosen.*

Is there any guidance available?

The most useful starting point is to consider the British Information Security Standard BS 7799 which was recently adopted as an international standard, ISO 17799. This standard, if properly applied, will provide for all your information security requirements. It covers ten areas to consider when reviewing your information security.

You choose which parts of the standard you apply and which bits you ignore. Naturally you would need to justify those areas you do not implement, if you choose to become ISO 17799 certified. These are management decisions, and could be based on, for example, cost, perceived lack of threat or other similar reasons.

Do I need help to do this?

Your company should be able to maintain the systems put in place without specialist help. However, it may be beneficial to have someone with whom you can discuss the issues, and provide expert advice and guidance as you implement your programme. Andy Taylor, of ValueAdding.com, can provide this for you and your organisation.