E-Business Security

Managing the risks of online business

David G.W. Birch
Director
Consult Hyperion
8 Frederick Sanger Road
Guildford
Surrey GU2 7ED

Telephone +44 (0)1483 301793
Fax +44 (0)1483 561657
E-mail dave.birch@chyp.com
Web http://www.chyp.com/

David G.W. Birch is a Director of Consult Hyperion—the IT management consultancy that specialises in electronic transactions—which he helped found after several years working as a consultant in Europe, the Far East and North America. A physicist by training, Dave has lectured on the impact of new communications technologies to MBA level. He is European correspondent for the Journal of Internet Banking and Commerce, a member of the editorial advisory the European Business Review and is a European Commission expert reviewer in the field of mobile commerce. Described by the UK newspaper The Independent in 2004 as a “grade-A geek”, he has written for publications ranging from The Guardian to the Parliamentary IT Review and is a media commentator on electronic business issues.

This version 10/18/03 10:28 am, 7948 words (26 pages)

An edited version of this guide was published by The Institute of Chartered Accountants (April 2005).
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFACE</td>
<td>3</td>
</tr>
<tr>
<td>1. DON’T PANIC</td>
<td>4</td>
</tr>
<tr>
<td>2. DEALING WITH RISK</td>
<td>5</td>
</tr>
<tr>
<td>3. BUSINESS THREATS</td>
<td>8</td>
</tr>
<tr>
<td>4. ELECTRONIC VULNERABILITIES</td>
<td>11</td>
</tr>
<tr>
<td>5. PRIORITISING COUNTERMEASURES</td>
<td>13</td>
</tr>
<tr>
<td>6. PRACTICAL STEPS</td>
<td>17</td>
</tr>
<tr>
<td>7. MANAGING THE SECURITY PROCESS</td>
<td>20</td>
</tr>
<tr>
<td>GLOSSARY</td>
<td>23</td>
</tr>
<tr>
<td>ABOUT CONSULT HYPERION</td>
<td>24</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>25</td>
</tr>
</tbody>
</table>
PREFACE

The risks associated with e-business are a combination of the characteristics of the new technology platforms—PCs, the web, GSM, digital TV and so on—and the problems associated with any other kind of business: fraud, human error, natural disasters, bad management decisions and so on. The channels for e-business clearly have specific challenges associated with them and business has yet to meet all of them. The recent US case of someone hacking in to a mobile operator’s servers to read customers’ e-mail [1] shows that even the biggest businesses are vulnerable, so it is no wonder that a typical business feels concerned.

They have every reason to be concerned. According to the UK’s National High-Tech Crime Unit (NHTCU), Internet crime cost UK businesses nearly £2.5 billion last year [2]. Industry surveys have shown for years that around a fifth of corporate IT spending is wasted and poor risk management is a big factor. Interestingly, the rise in outsourcing has been accompanied by increased risk of failure [3]. A third of UK companies are at risk from hacking because they have concentrated on ‘headline’ worries whilst ignoring basic security flaws [4]. An NHS Trust has gone back to pencil and paper to dispatch ambulances because the computer kept going wrong [5]. How are the public to know whether it is it bad software, disgruntled former employees or teenage hackers at fault?

The truth is that security problems are real, whether caused by errors or criminals, but they are not the reason that businesses appear to be losing the battle (with the average losses from worms, hacking, insider abuse and so on rising more than 15% per annum). The failure is a failure to think clearly about the risks to electronic business and what to do about them [6].

This short booklet aims to provide comfort to business managers. Its message is “don’t panic”. There are tools and techniques available to mitigate e-business risk and they can work well if they are handled in the right framework. One way of building this framework is through risk analysis and the booklet provides a high-level overview of risk analysis for organisations that interact with customers, partners and suppliers across electronic channels: the PC, the mobile phone, the interactive digital TV set-top box, kiosks and so on.

The goal of risk analysis is to bring together the threats to a business (eg, a competitor will discover a tender price and underbid) with the vulnerabilities of the new platform (eg, our e-mail server could be monitored by someone outside the company). Where a threat and a vulnerability coincide then there is a risk: by calculating the exposures associated with such risks and ranking them, it is possible to direct countermeasures expenditure to make it as efficient as possible.

Panicing about hackers is not the best response to security problems in an e-business. Kicking off an appropriate risk management process is.
1. DON’T PANIC

E-Business

It’s a natural human tendency to view new technologies in the light of existing knowledge, and therefore to project our fears on to these new technologies. In 1299, the citizens of Florence decided to abolish the use of Arabic numerals in commercial transactions because of the clear (as they saw it) danger of fraud that the use of such numerals would create. After all, it was difficult to amend a figure in Roman numerals by adding another digit whereas Arabic numerals plainly invite criminals to do just that. In other words, putting XC after IX isn’t the same as changing ‘9’ to ‘99’ [7]. In fact, businesses soon evolved tools to enable them to exploit the obvious efficiencies of the Arabic system while mitigating the fear of fraud (by adding a horizontal line after numbers, for example, just as we right ‘only’ after the sum on a cheque). Is the Florentine’s fear of counterfeit ciphers so different from ours about cyberspace credit card fraud? Is the e-business world really an expanding pit of nameless evils, or are we worrying about the “dark side” of the Internet simply because e-business is relatively new?

We tend to favour the latter view and advise organisations to develop business strategies that are rooted in reality, not newspaper headlines. These headlines can be pretty scary, and it’s important to observe that they are not all hype. Every time that customers (and finance directors) read a headline like “Big ID Theft in California” [8], to pick one at random, it chips away at their confidence in the medium. But what to do? The openness and flexibility that dog us so far as security is concerned are precisely the characteristics that make the Internet such an attractive place to do business.

It is unrealistic to try to create an e-business infrastructure that will never go wrong, whether using the Internet or anything else. Systems always fail, no matter how much expertise sits behind them. More realistic goals might be to:

- Reduce exposure to the level at which it can either be insured away or managed by some other technique.

- Ensure that when systems fail, they fail safe.

- Match the vulnerabilities and countermeasures. The old 80/20 rule applies: 80% of vulnerabilities can be covered by 20% of countermeasures, so do the simple things first (lock the door at night before you start worry about hackers).

So how do we reach these goals, starting from the moment when the Managing Director comes in with yet another hacking story torn from the Sunday newspaper and demands to know whether his business is safe or not? We use risk analysis to establish the situation and prioritise action and then we institute a security process to take care of the ongoing risk management for our e-business.
2. DEALING WITH RISK

To understand risk analysis, we need to understand risk. When discussing e-business security, we have a very clear definition: a risk is the overlap between a threat and a vulnerability. If there is a vulnerability in a system, such as there being no lock on my front door, but there is no corresponding threat (because my house is completely empty and there is nothing to steal) then it may make sense to leave the vulnerability in place rather than spend money removing it. Conversely, if there is a threat but no corresponding vulnerability then it is not worth losing sleep on the threat.

An interesting example came a couple of years ago when a couple of researchers at Cambridge found that someone with unchallenged authority in a bank branch who could get uninterrupted access to an ATM (eg, a bank manager) could, with a degree of technical knowledge of ATM hardware, cryptography and IBM software (eg, not a bank manager) obtain the PINs of cards used in that ATM after a couple of days “cracking time”. In summary then, a technologically sophisticated bank manager might be able steal a couple of hundred pounds a day (presumably only for a few days) from a few bank accounts. Yet this was reported by the newspapers as threatening the future of the financial systems.

Now, while it’s true that the old adage that if you really want to steal money from a bank then you should work for one applies, I would have thought that this particular scam would be some way down the “to do” list of criminal masterminds working for large banks. In particular, if you’re a bank manager that there must be a great many much better ways of stealing money. (To pick another random example, the head of private banking at one UK bank was sentenced to four years in jail for stealing £1.7 million in a wholly non-technological fraud uncovered entirely by accident [9].)

This stories illustrate a crucial point about business risk, e- or otherwise: the person most likely to get away with the money is not the bank robber, but the bank manager. The overwhelming majority of cybercrimes are inside jobs. The headline tells you that, for example, a man who illegally accessed other peoples online stock trading accounts has been sentenced to more than three years in federal prison. Looks like hacking: did he use keyboard sniffers, line tappers or database hacks? No, read a bit further down and you find (of course) that it’s just old fashioned fraud with a cyberveneer: he had friend who worked in a company payroll office who provided the names, home addresses and social security numbers he needed to log in [10].

Going On Line

When business moves to electronic channels, so that senior management no longer understand exactly how it all works, middle managers become a particular threat. The US Association of Certified Fraud Examiners (ACFE) say that fraud perpetrators are likely to be college-educated, married and have no criminal record. Incidentally, they also note that auditors discover less than half of frauds (47%), with accidents (32%) and tip-offs (27%) find most of the others. In fact accidents uncover frauds more often than external auditors and have almost as good a record as

Shifting from business to e-business means both new threats and new vulnerabilities, we must be careful to make sure that management understand both and understand both in context in order to make good decisions on exposure minimisation. There is a way of evaluating threats and vulnerabilities in order to allocate countermeasures expenditure in the most effective way to reduce exposure: it’s called risk analysis.

As an organisation we have carried out risk analysis for electronic systems as diverse as equities settlement, retail electronic payments and a manned space mission (true!), and we have seen that the 80:20 rule carries through: a few vulnerabilities account for the majority of the risks, so directing the budget at those vulnerabilities makes the most sense (even if they are unglamorous). While risk analysis for a big business with many systems may be complex, the risk analysis process will soon highlight a few key vulnerabilities and it makes sense to go ahead and fix them before waiting for the final results of the detailed analysis. Once the final results are in, then the sensitivity calculations (“if we spend £X on vulnerability Y, does total exposure fall by more than £X”) can proceed to bound the rest of the spending.

There are many different risk analysis techniques and you should choose one that is appropriate to your business: we use a proven technique, refined in–house, called Structured Risk Analysis (SRA) [12]. This employs structured analysis models to obtain semi–quantitative risk assessments that are suitable for a range of businesses. This is why we can confidently say “don’t panic”. If you do your risk analysis properly and allocate your countermeasures budget accordingly you can sleep comfortably at night!

**Security in Context**

Risk analysis, of whichever kind, is based on the principal concepts of threat, vulnerability, attack, risk and countermeasure. These concepts, as shown in Figure 1 applied to the e-business world, exist in one form or another in all risk analysis techniques.

A threat is something which will have an adverse effect on an organisation. A threat exists whether or not there are any practical or apparent ways in which it might ever be manifested. The threats to an IS are independent from the physical implementation of the IS. That is, whether your infrastructure is a single PC on your desk or a network of supercomputers around the globe, the threats to your business area the same.

A vulnerability is a characteristic of a physical system which, while being independent from any specific threat, allows (in principle) a threat to be exploited. Vulnerabilities are a property of the physical implementation of the technology and are independent from business threats.

Threats and vulnerabilities are divided into three categories for the purposes of analysis: confidentiality, integrity and availability. This time-honoured CIA classification, as it is called, is adequate for describing all of the various threats and vulnerabilities that can affect a business.
A risk is something which exists when a threat and a vulnerability overlap. That is, there is a threat to the business and a vulnerability which may be exploited to realise this threat. An attempt to exploit a risk—that is, to realise a threat—is called an attack and the person, agency or organisation attempting to exploit that risk is the attacker. Note that the same risk may be exploited by different attackers: in each case, this constitutes a separate attack. Note also that not all attacks are successful.

A countermeasure is something which reduces exposure, either by reducing the probability of loss (reducing vulnerability), the loss associated with a threat (reducing impact) or the loss resulting from attack (either by reducing the size of the loss or making it predictable—like house insurance). Remember that pointless countermeasures lose money just as effectively as a hacker stealing it over the web.

Figure 1. Risk Analysis Concepts.
3. BUSINESS THREATS

Identifying Threats

Threats are threats to the company business model, not its technology. Identifying threats, then, comes down to working through the business model to identify the threats to that model, classifying them according to the CIA model, labelling them so that they can be tracked and then assessing the level of the threat in terms of the organisation's potential loss (however measured) and the attackers potential gain. A simplified extract from a real threat catalogue is shown in Figure 2. Note that it is of no concern to the threat catalogue, or the business analysts putting it together, how an attacker might exploit any of these threats. What is important is that the threat catalogue is assembled methodically and presents an accurate picture and that all of the important threats are understood. Most of these, in our experience, will have nothing to do with disaffected teenagers lurking on the Internet.

<table>
<thead>
<tr>
<th>Inf. Asset</th>
<th>Information Asset Name</th>
<th>Threat ID</th>
<th>Description of Threat to Information Asset</th>
<th>Loss (L)</th>
<th>Gain (G)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Customer</td>
<td>I1</td>
<td>Customer Lost/corrupt</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>Customer</td>
<td>C1</td>
<td>Customer Disclosed</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>Customer</td>
<td>A1</td>
<td>Customer Not Available</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Supplier</td>
<td>I2</td>
<td>Supplier Lost/corrupt</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Supplier</td>
<td>C2</td>
<td>Supplier Disclosed</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Supplier</td>
<td>A2</td>
<td>Supplier Not Available</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>Sales Order</td>
<td>I3</td>
<td>Sales Order Lost/corrupt</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>Sales Order</td>
<td>C3</td>
<td>Sales Order Disclosed</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Sales Order</td>
<td>A3</td>
<td>Sales Order Not Available</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>Purchase Order</td>
<td>I4</td>
<td>Purchase Order Lost/corrupt</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>Purchase Order</td>
<td>C4</td>
<td>Purchase Order Disclosed</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>Purchase Order</td>
<td>A4</td>
<td>Purchase Order Not Available</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 2. Threat Catalogue.

This catalogue has been constructed from the organisational information model and the integrity threat (I), the confidentiality threat (C) and the availability threat (A) identified. Each information asset is already labelled (because of structured analysis) and so each individual threat is similarly labelled for cataloguing. So, information asset 3 (say) would have three entries in the threat catalogue: I3, C3 and A3.

The catalogue also contains the loss to the defender and the gain to an attacker. In this case, to avoid the difficulty of working with large numbers, a logarithmic metric (based on the FIPS metrics) has been used might be as follows: Loss or Gain amount less than £10, Impact Metric 0; Loss or Gain amount less than £100, Impact Metric 1; and so on.

The Enemy Within!

As noted, the most dangerous class of attackers (and the class that figures in the biggest exposures) is always those on the inside. Whether it’s a bus driver letting friends on for free or a corrupt middle manager authorising bogus invoices, they are the most dangerous because they know how the system as a whole works and not just how the security system works. It’s hard to
defend a system against people who are allowed to use it but abuse that privilege. The British
government was forced to shut down a £250 million system for managing training (“Individual
Learning Accounts”, or ILAs) because of widespread fraud [13]. Anyone with access to one
legitimate account number (ie, legitimate users, not hackers) could generate others and then
masquerade as students on the web site, fill out forms to indicate that training had been received
and sit back and collect money from the Government.

Ex-employees are another major problem. When business shifts from paper to web sites, it is
much easier for an employee to walk out the door with the entire business saved on his iPod
[14]. Of course they don’t even need to steal data: how do you make sure that ex-employees no
longer have valid passwords or access codes? At WTVT in Florida an employee noticed that a
number of computer files were missing: an investigation revealed that over a period of weeks,
the station’s newsroom computer had been the subject of repeated illegal access. A subsequent
police investigation led to the arrest of an ex-employee now working for a rival station!

Generally speaking, risk analysis will reveal that the largest exposures stem from risks that
combine internal attackers (most able to capitalise on a threat) with a small number of serious
vulnerabilities. Thus, when constructing the threat models don’t be seduced by the most exciting,
most technologically sophisticated threats and pathological vulnerabilities (“suppose a someone
with a telescope sees the secretary entering a password…”) at the expense of those likely to lead
to maximum exposure (“suppose a corrupt account manager and his friend at the bus
company…”).

Case Study: A Manned Space Mission

We were retained by an international space agency to carry out risk analysis for a manned space
mission. In this kind of system, financial loss is not the measure of exposure: human safety is
paramount, so the relevant exposure metric is the danger to human life. In this case, because of
the difficulty of assigning values to safety–related issues, the client chose a 3–point measurement
scale (low, medium, high) for “costs” and a 5–point scale (slight through to extreme) for
exposures.

As you can imagine, this was a highly distributed system. Most of the users (in University
departments: not the most secure computing environments!) were to be connected via a LAN to
user site systems and from there via public networks to mission control. Controllers would
access the mission control computers directly over a LAN. A satellite link would provide
communication between mission control and the spacecraft master computer. Status and results
would be sent to mission control and user sites respectively, via the satellite link. Controllers
could control the systems directly, schedule system activities and update systems software. Users
could only schedule payload activity, which has to be checked in advance by mission control.

To give you a feeling for the results of the risk analysis, it was determined that the risk with the
greatest associated exposure was for a false onboard program to be created at mission control.
The most likely attacker was a disaffected employee, whilst the cost of exploiting mission
control’s vulnerability was low.
Therefore it was decided to improve the integrity of the mission control computers by implementing a rigorous security policy at the same time as improving the availability of the mission control computers by implementing a “hot standby” fault tolerant machines. We also recommended some inexpensive cryptographic tools to improve the confidentiality of communications between certain computers.
4. ELECTRONIC VULNERABILITIES

Finding Vulnerabilities

Vulnerabilities are an inevitable property of any system. They are things that can go wrong with technology: not necessarily because of organised crime or denial-of-service (DoS) blackmailers. If there is one single category of vulnerability that stands out in e-business, it is software. Two examples serve to make the point.

The Bank of New York (BoNY) specialises in settling transactions in Government securities. It takes securities from the selling bank, pays for them, passes them on to the buying bank and collects the money. On November 21st 1985 a small software error caused BoNY’s computers to stop passing them on the purchasers and collecting the money. By 11.30am, BoNY’s overdraft at the Federal Reserve had reached $12 billion (I imagine they got a call from their personal banker by this time) and the fault was not rectified until the following day, by which time it stood at $44 billion and was threatening to disrupt the financing of the US budget deficit. The error cost BoNY $4M in interest charges [15].

Closer to home, a software upgrade that went wrong took down the Department of Work and Pensions entire network in November 2004, preventing them from processing new claims. This was reported as the biggest computer crash in the history of the UK government, since about a hundred thousand desktops were disrupted [16]. This, again, shows that systems are not just about hardware and software: they are about contingency plans, backup and recovery tactics, fallback and other factors, all of which have to be taken into account to assess the vulnerability of organisation.

Assessing Vulnerabilities

Vulnerabilities are catalogued against the networks and computers in the technology model. Each physical asset on the technology model (either a data flow or a data store) is already uniquely labelled, so each of the vulnerabilities will be similarly labelled. Three vulnerabilities are assigned to each physical asset: the integrity vulnerability (I), the confidentiality vulnerability (C) and the availability vulnerability (A). So, physical asset 1.3 (say) would have three entries in the vulnerability catalogue: I1.3, C1.3 and A1.3. In order to later calculate exposure, we need to capture two parameters of each vulnerability: the cost of exploiting that vulnerability (C) and the probability of exploiting the vulnerability successfully (P). Costs are described using the same metric as for threat impact whereas the probability of successful attack is indicated using a similar logarithmic metric (-3 very unlikely, -2 unlikely, -1 possible, and so on). Table 1 shows a vulnerability catalogue being assembled.
<table>
<thead>
<tr>
<th>AID</th>
<th>System</th>
<th>Vul. ID</th>
<th>Description</th>
<th>Cost</th>
<th>Prob.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Web server</td>
<td>I1</td>
<td>Server tampered</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C1</td>
<td>Server accessed</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A1</td>
<td>Server down</td>
<td>2</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>SQL Server</td>
<td>I2</td>
<td>Database tampered</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C2</td>
<td>Database accessed</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>DMZ Ethernet</td>
<td>I3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Building a Vulnerability Catalogue.

Although there may be a great many technology assets (depending on the level to which the technology model has been developed, of course) it is usually straightforward to assign the costs and probabilities associated with the vulnerabilities because they are generic—it takes the same effort to tap a web session whether the network is being used for credit card verification or playing games—and the vulnerability catalogue can be constructed without complication.

**Case Study: Electronic Tickets**

For a transit operator we carried out risk analysis of a proposed electronic ticketing scheme for cross-operator use. Around the world, mass transit operators are beginning to use electronic ticketing systems to both expand their markets beyond transportation and to implement additional electronic business functionality.

The issues they face are representative of the challenges faced by many businesses moving from a tried and tested paper-based system to an online electronic system and (since everyone understands what a train ticket is!) make for an interesting case study. Unlike the paper system, the electronic system may have a future that takes in new business, partnerships and opportunities so it needs to have a security architecture that can evolve.

One particularly interesting issue is that of anti-fraud countermeasures. There are a number of balances to be found. Tickets must be secure, but they must also be inexpensive. The web site must be easy to use, but it must deter fraud (there was a particular problem arising from the purchase of expensive tickets with fraudulent credit cards). The tickets must work, right now, but must be open to extension.

Risk analysis provided a much better framework for discussing, exploring and assessing these balances than whiteboard designs or potentially seductive prototypes. The operator was able to construct a sensible roadmap, based on the right standards, and justify technology choices in a framework and language that allowed for real interaction with business units.
5. PRIORITISING COUNTERMEASURES

In the case of electronic channels, the countermeasures that can be employed to reduce risk are well–known and an array of techniques are available, but high countermeasures expenditure on every possible contingency is out of the question in most organisations: yes, the web server may be destroyed by an asteroid strike, but relocating to Mars may be a tad beyond budget. Therefore, expenditure must be directed to reduce corporate exposure to e-business in the context of two key questions:

- How much is it appropriate to spend on countermeasures?
- Where should this spending be directed?

There are insecure systems in operation which may cost businesses millions of pounds if the insecurities are exploited. There are also systems with inappropriate and over–expensive security countermeasures, which are just as responsible for losing money. By way of illustration, suppose a risk loses a business £10,000 per year. It is clearly inappropriate to spend £200,000 to close this risk, since the same investment would yield more than enough to cover the losses if invested in some other way.

Using risk analysis, we can calculate where to invest countermeasures. Remember that risk exists where there are a threat and a vulnerability that coincide with a shared attacker. The Risk Catalogue is formed by examining each threat in the Threat Catalogue and matching it against the vulnerability catalogue. This results in a Risk Catalogue, as shown in Table 1.

<table>
<thead>
<tr>
<th>RID</th>
<th>Threat</th>
<th>Vuln.</th>
<th>Description</th>
<th>Loss</th>
<th>Inc.</th>
<th>Prob.</th>
</tr>
</thead>
<tbody>
<tr>
<td>I1-1</td>
<td>I1</td>
<td>I1.1</td>
<td>Incorrect customer details inserted in SQL database</td>
<td>3</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>I1-2</td>
<td>I1</td>
<td>I1.2</td>
<td>Corrupt customer details on SQL database</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>I1-3</td>
<td>I1</td>
<td>I1.3</td>
<td>Incorrect customer details inserted in SQL database</td>
<td>3</td>
<td>0</td>
<td>-2</td>
</tr>
<tr>
<td>I1-4</td>
<td>I1</td>
<td>I1.4</td>
<td>Corrupt customer details on SQL database</td>
<td>2</td>
<td>0</td>
<td>-2</td>
</tr>
</tbody>
</table>

*Table 2. Building a Risk Catalogue.*

The step–by–step cross–referencing used to build up this catalogue is not complex because of the structured nature of the underlying models. The Attacker Catalogue is similarly simple because it general only needs broad categories. While the scope of deliberate attacks can be quite wide, as they cover fraud, malicious damage—even “electronic picketing” by activists or deliberate DoS by blackmailers—whereas accidents and natural disasters are much easier to enumerate. To
reflect this, the class of deliberate attacker can be subdivided into a number of different attackers where the potential of attack varies greatly (because of very different gains and so forth) as shown in Table 3.

<table>
<thead>
<tr>
<th>Class</th>
<th>AID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural</td>
<td>N1</td>
<td>Fire/Flood</td>
</tr>
<tr>
<td>Accident</td>
<td>A1</td>
<td>Anyone</td>
</tr>
<tr>
<td>Deliberate</td>
<td>D1</td>
<td>Competitor</td>
</tr>
<tr>
<td></td>
<td>D2</td>
<td>Vandal</td>
</tr>
</tbody>
</table>

*Table 3. A Sample Attacker Catalogue.*

For each risk in the risk catalogue, we define one attack for each attacker type: again, a simplification, because different types of hacker might out for different things (some might just want to cause mischief, some might want to steal money). Then a frequency of occurrence (O) must be assigned to each attack. As in the case of threat impacts, we have used a general purpose logarithmic metric for O (again, very simplified for this example):

- For Natural attackers, O is -1 (that is, we assume a natural disaster once every ten years)
- For Accidental attackers, O is 0 (that is, we assume that accidents happen once per year)
- For Deliberate attackers we have two metrics: for Competitors, O is P+I (that is, the greater the incentive the greater the frequency of attack) but for Vandals, O is P-C (Vandals are assumed to have no gain, only costs).

Now, since for each of the attacks in the Attack Catalogue we know the frequency of occurrence O (from our calculations) and the impact (from the threat catalogue), we can define the exposure (E). The simple metrics used here mean that we can calculate the annual exposure to a risk as the sum of the impact (of the associated threat) and the frequency (of the associated attack), so that \( E = L + O \). Given the logarithmic nature of the exposure so calculated, we can define the exposure for each risk as the highest exposure of any of the attacks associated with the risk.

This leads us to the final catalogue of interest. We sort the risks by exposure and call this the Exposure Catalogue, as shown in Table 4.
Table 4. Building a Risk Catalogue.

<table>
<thead>
<tr>
<th>RID</th>
<th>Description</th>
<th>Prob.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RC1-1</td>
<td>Competitor accesses customer database</td>
<td>-1</td>
</tr>
<tr>
<td>RC5-1</td>
<td>Competitor accesses delivery/invoice details</td>
<td>2</td>
</tr>
<tr>
<td>RI2-4</td>
<td>Incorrect customer details added to proposal</td>
<td>-2</td>
</tr>
<tr>
<td></td>
<td>management systems</td>
<td></td>
</tr>
<tr>
<td>RI7-5</td>
<td>Incorrect supplier order placed because of tampering</td>
<td>-2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In this example, this highest exposures relate to the disclosure of customer records (i.e., a competitor reading customers’ orders). This is as would be expected, since for our example company it is competitors stealing orders that is the biggest problem. The value of the highest exposure, 6, indicates that the company has a current exposure of around £1M per year.

Now we have basis for deciding whether to spend money on a countermeasure or not.

What Actions?

Once exposures have been determined, the structured catalogues allow the Risk Manager to work back to the Vulnerability Catalogue to determine where countermeasures expenditure would be best directed. The Risk Manager has three basic options with regard to each exposure: acceptance, insurance or avoidance (by countermeasure procurement.) The choice depends on the size of the exposure and the likely frequency of successful attacks, as shown in Figure 8.

![Figure 3. Options for Actions.](image)

Case Study: Smart Credit Cards

Systems for billing, payments and account management need risk analysis. In these cases, organisations such as banks understand both the financial losses that may occur if attackers get into an electronic payment system but they are also sensitive to the reputational losses that may follow. Therefore they need risk analysis to
We carried out a risk analysis on a new smart credit card—smart in the sense of using smart cards—for an international financial services organisation. This was their first smart card product for consumers anywhere in the world so in addition to the financial exposure it was important to minimise reputation exposure.

Our risk analysis revealed that the countermeasures in place in both the card and the processing systems had been carefully designed and properly implemented and exposure was minimal. What we did discover, however, was that the system for issuing the card to consumers had not been through the same rigorous design and implementation process and that significant exposure remained. Subverted employees of the company chosen to manage the issuing process could have created bogus cards or engaged in other (more complex) activities that could have resulted in substantial loss. A few simple changes to the business model and improved authentication in the technology model were all that was necessary to bring exposure down to manageable levels.
6. PRACTICAL STEPS

Root Causes

Is it realistic for an e-business to expect technology to minimise their risks? As you’d expect from a consultancy, the answer is “yes” and “no”. That’s because risk is a big issue with many facets (so “no”). On the other hand, many types of risk share the same root problem (so “yes”).

For a great many businesses, this root problem is identity: how do you know who the person in the shop, on the end of a phone, sitting in front of the TV and accessing your web page is? If technology could help to attack this fundamental issue, then many kinds of fraud could be substantially reduced.

There’s no denying the scale of the problem. In the very current and visible case of payment cards, identity-based fraud (the fraudulent opening of accounts using other peoples’ details or the unlawful appropriation of other peoples’ accounts) grew by nearly half last year and the use of fraudulent credit cards online drives merchants to distraction. Software solutions can help, but they are tackling the symptoms, not the problem. There is no proper identity infrastructure and therefore no proper identity management: most businesses let customers, partners and suppliers in with passwords.

Passwords are not really security: it’s just too easy for people to steal them, guess them or “socially engineer” them. Not only are they insecure, they are expensive. Forrester Research reckon that the average “large company” spends $1 million per annum on recovering lost passwords and login names. The dependence on passwords has also led to entirely new vulnerability, phishing. Who hasn’t received an e-mail purporting to come from their bank, eBay or Paypal, inviting them to log in at an utterly bogus (but convincing) web site! As the old saying goes, on the Internet no-one knows you’re a dog. Taking care of this one single element of online security would do more to minimise the exposure of e-businesses than anything else. That’s why the issue of authentication is so important and why it represents the single most important challenge for most e-businesses.

Authentication Strategies

So how can technology tell us who someone is? The technology getting the most media attention in this context is biometrics. Here, the hype is some way ahead of the reality. The idea that someone might simply walk into a bank and use their fingerprint to obtain money is far-fetched: fingerprint matching is imprecise, and inexpensive fingerprint readers are too easy to fool with phoney fingers (and even fingers from corpses) for population-scale applications. Even in smaller systems, fingerprints can give a false sense of security. In one prison in Scotland, mechanical locks were replaced by fingerprint readers so that prison officers’ fingerprint could lock and unlock prison doors. However, problems arose after a prisoner demonstrated to wardens that he could get through the doors at will and it was then discovered that other prisoners (including murderers) had been doing the same for some time. Instead of
fixing the state-of-the-art technology, prison governors have decided that it is more cost-effective to get rid of it and return to the system of every officer having his own key [17].

While fingerprints may be imperfect as an identifier, however, they are excellent as an authenticator. They work very well in a system of one-to-one matches, where a smart ID “card” (which may be a card, or a keyfob or a watch or anything else) holds a biometric template that is checked locally against the biometric data of the carrier. In this case, the fingerprint template would only be stored in the ID card and not by the bank or anyone else, and it’s the card that checks the customer’s fingerprint against the template.

This is what security experts call “two factor” authentication, because a person needs both the card and the fingerprint to make a transaction. Since such cards would still carry the PIN as well, the system would deliver the “three factor” authentication beloved by security experts:

- Something you have (the card);
- Something you know (the PIN);
- Something you are (the fingerprint).

This would allow organisations to create risk-matched payments processes for optimising customer contact experiences while simultaneously reducing fraud. The retail payment example is easy to visualise: perhaps for a small transaction you simply wave your keyring by the till, for larger transactions you punch in a PIN and then wave your keyring by the till and for the largest transactions you place your keyring on the till and put your finger on the fingerprint scanner.

The smart cards already being issued by banks can help others to tackle fraud as well and they are being spurred on right now because of another fraud epidemic: phishing (obtaining personal details, especially financial details, using deceptive e-mails and web sites). Phishing is another manifestation of the underlying problem of authentication to online services being so weak, of nothing more than basic password authentication. The very fact that phishing sites work at all proves that the authentication (in both directions) is effectively non-existent: the fact is that customers need to have as much assurance that they know who they’re dealing with as the service provider does about who is logging onto its service.

As Bill Gates said back in 2000, passwords are the weak link and the industry needs to move to smart cards. For most e-businesses, effective identity and authentication will be the best value for the countermeasure dollar.

**Identity Management**

As noted previously, for many businesses today a substantial proportion of their overall exposure (whatever the electronic channels in use) comes from poor identity management and poor authentication. In the current environment, it makes sense to begin tackling these issues as the risk analysis is performed so that you can take action sooner rather than later.
The limitations of “one factor” authentication are evident and are in sharp focus in the banking world. The use of one factor (the card) in the physical world has led to fraud of many kinds and UK banks and retailers have spent more than a billion pounds moving to two factor (“chip and PIN”) authentication. Similarly, the use of one factor (username and password) authentication for home banking has led to problems.

Against this, it is not enough to assume that customers can be educated and then relied on to recognise fraud when it happens. It’s just impossible to stop this sort of fraud without better authentication.

Many e-business vulnerabilities reduce to the pressing problem of identity management and authentication, and hence these are high up the list of priorities for IT spending. Better identity management together with two factor authentication is likely to have a major impact on exposure minimisation for most businesses.

**Case Study: Boosting Authentication**

We are an SME and we depend on our intranet to function. The intranet carries our most business-sensitive information: client details, proposals in progress, project tracking, financial data of many kinds, lead management and so on. We didn’t need to complete detailed risk analysis to identify that moving our staff on to an intranet meant dealing with basic vulnerabilities, especially since we need our staff to be able to access the intranet over the public internet. Many of our consultants spend much of their time working on client premises and if they cannot get access to the intranet it’s a real problem.

We installed digital certificates on our consultants laptops. Almost all web servers and web browsers implement a protocol called Secure Sockets Layer, or SSL (it’s where the padlock in the corner of your browser comes from when you access a secure web site). With the right digital certificate, a laptop can connect to our intranet servers with an encrypted and authenticated link. This end-to-end solution means that we don’t need to worry about the physical network security at all.

But what if the consultant doesn’t have the laptop? Perhaps they are using a client PC, or their laptop is broken so they’re using a temporary replacement, or perhaps something has gone wrong with their software and the digital certificate has been corrupted or lost? Then we use simple, two-factor authentication. The consultant comes to the web site and enters their staff number. Our system knows their mobile phone number, so given the staff number it can send a text message containing a one-off password. The consultant enters the password and is given encrypted access. A competitor trying to gain access to our pending proposals file would have to know a consultant’s staff number and steal their mobile phone (without the consultant noticing) and makes the exposure manageable in the context of other business risks.
7. MANAGING THE SECURITY PROCESS

Create a Process

Bruce Schneier, the author of *Applied Cryptography* and *Secrets & Lies*, is very fond of saying that security is a process, not a product, and he is of course correct. It’s not all about technology, although many seem to think it is. Three-quarters of the respondents in a recent UK poll of senior executives had already experienced unexpected availability in business critical systems, yet half still saw availability as an IT responsibility. Experts agree that electronic risk management cannot be the sole remit of IT: it should be an element of business process and it should be an ongoing process.

So make it someone’s problem. Put someone (not from IT) in charge of minimising e-business risk. And help them to kick the process off. When starting with a “blank sheet” a comprehensive risk analysis will have to be performed so the process will take real resources to get underway but the initial risk analysis must then be maintained to reflect:

- Reduction in vulnerabilities by procurement of countermeasures
- Changes in the information or business models as the business changes
- Changes in the physical model (new computers or networks, etc) supporting the same information (hence changes to the vulnerabilities).

Once the risk analysis has been performed, a plan should be constructed to procure the countermeasures required to mitigate the most important threats. Obviously, this will be subject to budgetary constraints. The appropriate size of this budget can be determined by the relative magnitude of the information risks compared to the business’s other risks. Help your e-risk manager to keep the process moving by making sure they get the right support:

- Maintaining the threat catalogue needs the input of business managers. Many of threats—failure to comply with Sarbannes Oxley, for example—can only be understood and quantified by staff in business units, not IT.
- Maintaining the vulnerability catalogue need not be arduous. Most of the vulnerabilities will be generic to the technology employed (eg, PCs or mobile phones) and the catalogue will only need significant revision when there is a technology change.

Help your e-risk manager to communicate the success of the process. Not simply for personal glory, but because the perception of detection is a significant deterrent: companies should publicise results of investigations, not hide them [11].
Business Process

Don’t forget that the implications go beyond IT. Spending money on technology countermeasures may be part of the implementation, but it is not the whole solution: there will undoubtedly be changes to the business as a result. Companies don’t have their own security guards (they use security companies), they don’t have their own armoured cars (they hire them) and they don’t do their own auditing (they are legally required to have someone else take a look). Perhaps if more companies were to view electronic security as a real business process and outsource it in the same way then it would get taken seriously instead of being left to someone in the IT department in their spare time: certainly, for many SMEs, it will be vastly more cost-effective overall to outsource components such as web sites and e-mail servers (as shown in Figure 4, using our own architecture as an example) to organisations able to make the investment in firewalls, back-up sites, load balancing systems, virus scanners and the rest.

Figure 4. An Example E-Business Architecture.

Avoid Paralysis

A final practical point. You don’t have to wait until the detailed risk analysis is complete before you take action. Some early, large exposures are bound to be revealed and you should begin to deal with them as soon as they are recognised. It is often the case that big chunks of e-business
exposure trace to basic technology vulnerabilities and these need addressing with basic countermeasures.

Most of these basic countermeasures are now quite standard and there is no need to labour the point on their necessity. Things like firewalls, virus scanners and spam filters should be part of your IT infrastructure already. In many companies, they are. At the time of writing, more than three-quarters of all Internet e-mail traffic is spam and another 2% of it is viruses yet most companies continue to use the Internet successfully. There’s no excuse for doing nothing.
GLOSSARY

ATM  Automated Teller Machine
CIA  Confidentiality, Integrity and Availability
DoS  Denial of Service
DMZ  Demilitarised Zone
FIPS Federal Information Processing Standards
SME  Small to Medium-Sized Enterprise
SRA  Structured Risk Analysis
SSL  Secure Sockets Layer
VPN  Virtual Private Network
ABOUT CONSULT HYPERION

We are an independent IT management consultancy with a global client base. Focusing on secure electronic transactions, we help organisations to bridge the gap between business and technology. We have applied our expertise to a wide range of systems and applications, including national ID cards, mobile top-up, retail payments and Customer Relationship Management.

We provide practical advice at every stage in the project life cycle covering:

- Evaluation of new business concepts
- Development and Implementation of new products and services
- Ongoing development and improvement of existing systems

Our aim is to assist our clients in reaching their goals in a timely and cost-effective way. We work in four main sectors:

- Financial Services
- Retail
- Public Sector
- Telecommunications, Media and Technology (TMT).

We support the deployment of practical solutions using the most appropriate technologies. We have world-class expertise at every step in the transaction value chain:

- Authentication using technologies such as smart cards, RFID and biometrics
- Access Devices, such as set-top boxes, PCs and mobile phones
- Digital Mobile Networks, such as those supporting digital TV and the Internet
- Transaction Services, founded on the concepts of digital money and digital identity
- Applications ranging from retail electronic payments (EMV chip and PIN) to electronic immigration control
REFERENCES


11. Zikmund, P. 10 truths you need to know about fraud in Strategic Finance (1st May 2004).


