M. ERIC JOHNSON

A broader context for information security

The goal of effective risk management for information technology is not the elimination of security failures, but rather reducing their cost while empowering the business to take appropriate risks

The risks of serious information security failures are all around us. Breaches, such as teenage hackers and e-mail viruses, were once a nuisance only for information technology professionals, but now they have become a significant risk for executives and can threaten intellectual property and brand equity. Each new lapse in security, highlighted by glaring media coverage, amplifies consumer awareness and concern.

The June disclosure by MasterCard that 40m of its credit and debit card account details had been exposed is yet one more indication of the breathtaking scale of the problem. Certainly, the growing fear of identify theft is a matter of concern for executives in industries that interact directly with consumers. In a recent survey we conducted in conjunction with the Merchant Risk Council, we found that over 90 per cent of retailers agreed that consumers make purchasing decisions based on their trust in the company's ability to secure their data. And almost 90 per cent felt that information security is or will become a point of competition in the retail sector.

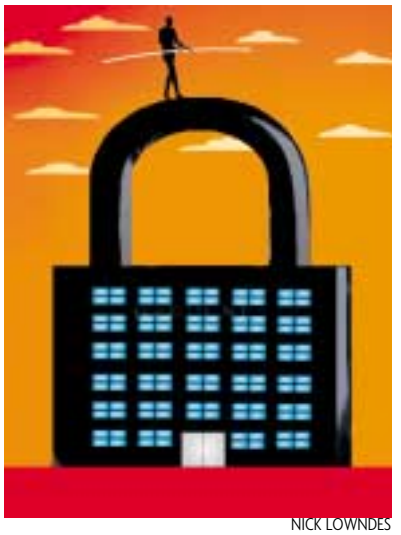
Information security is not just an issue for retailers and banks – all companies face new risks, ranging from industrial espionage to sabotage. Compounding these concerns, compliance fears generated by Sarbanes-Oxley and the forthcoming Basel II accord have fostered an environment of risk aversion inside many organisations.

Of course, there are plenty of risks to fear. The process of opening companies to the internet has exposed a multitude of software vulnerabilities, especially as many older systems were not developed with security in mind. Building stronger walls around enterprise systems can help to keep out some unwanted visitors, but those clever invaders or disloyal insiders who find their way into the fortress discover a treasure trove of information once they have gained access.

To make matters worse, many risks lie deeply hidden within the extended enterprise. While most large companies have taken significant actions to beef up their own internal security, their smaller partners often harbour risks that open the entire enterprise to vulnerability. Every day, business partners take unseen risks and, when partners experience security failures, it has the same devastating impact. In the case of MasterCard, the loss arose out of a security breach at CardSystems Solutions – a small, private payment processor with only about 100 employees. CardSystems quickly felt the pain of the mistake as both Visa and American Express promptly pulled their business, pushing CardSystems into financial crisis. Yet the fact that the problem was not within Visa or MasterCard made little difference to consumers, who rightly saw the problem as the responsibility of the credit card companies.

Even in my business, MBA education, a small company's problem quickly became a serious headache for deans of the world's top schools. The story should sound achingly familiar to IT executives. In the process of moving to the web, many schools outsourced their online application system. The leading company, ApplyYourself, had a ready-made solution that was superior to anything most schools could develop in a cost-effective way on their own. Applicants in their twenties, who grew up with the internet, loved the convenience and quickly shifted to the online solution. However, when a disgruntled Harvard applicant found a flaw in the security of ApplyYourself's system, he decided to post his discovery on the web. By following his simple instructions, average MBA applicants turned themselves into cyber hackers, and a number of them were able to see the outcome of their application before the official announcement. While the security hole was plugged within hours, schools from Harvard to Stanford and Tuck all felt the public embarrassment. As global brands with rich histories, they had much to lose.

Certainly, the failure was a business crisis for ApplyYourself – its CEO spent the spring quarter scrambling from school to school trying to head off a mass exodus.



NICK LOWNDES

The lesson is clear – managers must consider the risk management practices of their partners. Where does sensitive data flow when it leaves the enterprise? How is it protected and what are the risks? More importantly, do those partner companies have the right incentives to make the appropriate security investments? In short, managers must factor their partner's risk into their own risk portfolio.

The escalation of security breaches and the painful surprise many executives feel when a failure occurs in their business have brewed a culture of fear within many organisations. Vendors within the security industry have quickly capitalised on this fear along with the confusion around new compliance measures, such as Sarbanes-Oxley. But before tossing money at a cure in the hope that it will eliminate these new risks, managers should first work to incorporate information risk into an overall enterprise risk management strategy.

Like any other risk within the company, security risks must be identified and balanced against the benefits and costs of mitigation. Unfortunately, in contrast to many other business risks, the discussion about information security risk has focused solely on the negative experiences. Of course, no one likes bad outcomes. A hurricane, like a security failure that exposes sensitive customer information, results in damage and cost. However, in other areas of business, risk is associated with return – higher risks yield higher returns. This is also true for information security risk.

Too often, IT risks arise from sloppiness or corner-cutting, such as the failure to follow best software development practice or to test and audit new systems. In some instances, this notion is true. However, many IT risks occur within the context of a larger business strategy with associated rewards. For example:

- Working with a small innovative start-up company whose promising software solution could generate significant returns, but could also harbour the associated risk of the small company's IT environment
- Starting or acquiring operations in low-cost countries where the infrastructure is less secure
- Outsourcing business processes to suppliers with lower-cost structures but unknown or hard-to-monitor security practices
- Exposing internal business data to customers and partners to help with the creation of new services or reduce operating costs.

All of these create security risk, even with the best practices. Becoming aware of the risks is just the first step in building an effective management strategy. In our survey of retailers, over 85 per cent said that the level of information security offered by

M. Eric Johnson is director of the centre for digital strategies at the Tuck School of Business at Dartmouth College.
m.eric.johnson@dartmouth.edu

their suppliers was important to them. Yet we find that companies in every industry are struggling to develop effective ways to measure and manage security risk across their extended enterprise.

A simple way to reduce security risk is to limit business innovation – to avoid partnering, pull systems offline and lock down the fort. That is a serious mistake. Instead, risk should be balanced with reward. Embedding IT risk into your overall enterprise risk management strategy implies establishing a risk posture that does not seek to eliminate security risk, but rather manages it.

The key is first to understand the vulnerabilities, threats and consequences. Vulnerabilities are areas that can be exploited by malicious individuals or organisations. Examples could include poorly maintained software (such as failing to patch known security holes), poor security practices (such as inadequate password and identity management), or the exposure of older systems with unknown security to the internet.

Given these vulnerabilities, what are the threats? Are there outsiders who are motivated and capable of exploiting the vulnerability? Or are there insiders who may be tempted to steal intellectual property? Finally, if the security was breached, what are the consequences? Would they be primarily internally observed or would they impact external groups, such as customers or business partners?

Internal failures, like viruses, generate real operational costs for the IT department but rarely put the company into a catastrophic tailspin. On the other hand, external failures, such as a breach of customer information, can be much more painful, warranting far greater attention.

To manage risk in the most effective way possible, companies should include information security in the broader process of business risk management, where the board of directors governs the company's overall risk posture. This same process must also be applied to business partners. For many companies, measuring supplier risk will require new tools for supplier security qualification. Like those tools used to assess a supplier's product quality, supply chain reliability, or its long-term financial viability, suppliers should be qualified using a technical assessment of security and an assessment of the supplier's information risk management practices. Risks of working with a new partner can then be balanced against the benefit that the partner delivers.

Most importantly, managing information risk is everyone's responsibility – not simply the job of IT executives. Rather than viewing IT executives as security guards, technology-savvy executives – from corporate directors to line managers – should act as consultants to the entire organisation. CIOs with strong business and technical skills are uniquely qualified to help educate the organisation and chart a course to bring IT risk into the overall risk management strategy. Bringing IT into the enterprise risk management strategy will not only protect against catastrophic operational surprises, but will empower managers to seize the exciting opportunities before them.

John Hull and Alan White survey the fast-developing market for credit derivatives

New layers of protection

In recent years, new instruments, known as credit derivatives, have emerged for managing credit risk. In the late 1990s, the International Swaps and Derivatives Association produced a standard contract to facilitate trading in credit derivatives and, since then, the market has grown rapidly. In 2000, the total notional principal for outstanding contracts was about $800bn. Now, it is estimated to be over $5,000bn.

Credit derivatives allow companies to trade credit risks in much the same way that they trade risks associated with exchange rates or interest rates. A bank used to be able to do little when it had made a loan except wait and hope for the best. Now, it can actively manage its portfolio of credit risks. It can choose to keep some risks and to buy protection for others. It can also take on the credit risk of a company (and be reimbursed for doing so) without lending money to the company or entering into contracts of any sort with the company. This gives banks more scope to diversify credit exposures.

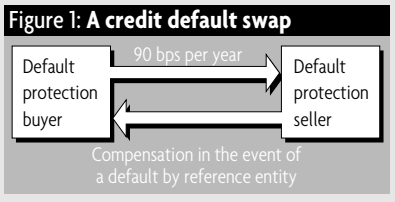
Credit default swaps

The simplest type of credit derivative is a credit default swap (CDS). An example is shown in Figure 1. Suppose that the notional principal is $10m and the contract lasts five years. The default protection buyer pays 90 basis points (or $90,000) per year to the protection seller to buy insurance against a default by the reference entity during the five years. The reference entity is typically a company or country.

The basis points paid per year by the default protection buyer is known as the CDS spread. If the reference entity is an AAA-rated company, the CDS spread is likely to be quite low (perhaps 20 basis points per year). As the credit quality of the reference entity declines, the CDS spread increases. In extreme cases, it can be several thousand basis points.

If there is no default by the reference entity, the CDS spread is paid for five years by the protection buyer and the protection seller does not have to pay anything. If there is a default within the five-year period, the payments from the protection buyer to the protection seller stop, and the protection seller has to pay the protection buyer $10m in return for the bonds issued by the reference entity that have a par value of $10m. Typically, a company's bonds are worth a lot less than par immediately after a default, so a default is quite costly for the protection seller. Sometimes, deals are structured so that, instead of the bonds changing hands, there is an equivalent cash payment from the protection seller to the buyer. Note that there is no requirement that the protection buyer owns bonds issued by the reference entity at the time a CDS is initiated.

Figure 1: **A credit default swap**



Suppose that the yield on a five-year bond issued by the reference entity is 5 per cent and the credit default swap spread is 90 basis points as in Figure 1. By buying the bond and default protection, an investor earns 5 per cent and pays 0.9 per cent to obtain a net return of 4.1 per cent. This return is almost risk-free. For there to be no arbitrage, 4.1 per cent should be the five-year risk-free rate. This shows that the credit default spread should be approximately equal to the spread of the reference entity's bond yield over the risk-free rate, and in practice, this is the case. Five-year credit default swap spreads are very close to the excess of the yield on five-year bonds issued by the reference entity over the five-year swap rate.

Credit derivatives have created a shift in the type of entities that bear credit risk in the economy. Banks have become net buyers of default protection and insurance companies have become net sellers. The result is that the financial institution bearing the credit risk of a loan is often different to the institution that did the original credit checks. Whether this proves to be good for the overall health of the financial system remains to be seen.

Portfolio credit risk

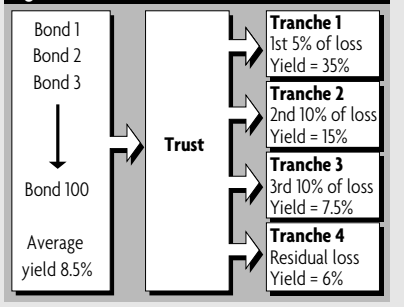
There are many variations on the standard plain vanilla credit default swap, but the most interesting recent developments in the credit derivatives market concern instruments that depend on the credit risk of a portfolio rather than a single reference entity. The traders of these instruments are concerned with the level of defaults in the economy as a whole. Consider a bank that has a well diversified portfolio of loans. If it buys protection against defaults on a similarly well-diversified portfolio, it has a hedge against the adverse impact on its bottom line of a high default rate in the economy.

To facilitate trading, a number of standard portfolios has been developed. The CDX IG portfolio consists of 125 North American investment grade bond issuers. The iTraxx portfolio similarly consists of 125 European investment grade names. These portfolios do not remain constant over time. For example, when a company in the iTraxx portfolio becomes non-investment grade or defaults, it is replaced by another company that is investment grade. There are indices associated with the portfolios. Suppose that the five-year iTraxx index is 45. This means that, in a single transaction, a portfolio of 125 five-year credit default swaps could be purchased on the companies that are in the index for 45 basis points per company. As with a CDS, the purchaser is not required to own any of the bonds on which protection is being provided.

A popular product is known as a collateralised debt obligation (CDO). This is a way of creating securities with widely different credit risk characteristics from a portfolio of bonds. Figure 2 shows an example of a cash CDO. It is created from a portfolio of 100 bonds, each having a notional principal of $1m. The losses arising from defaults on the bonds in the portfolio are distributed to tranches. Tranche 1 has a principal of $5m and is responsible for the first 5 per cent of losses on the portfolio; Tranche 2 has a principal of $10m and is responsible for the next 10 per cent of losses; Tranche 3 has a principal of $10m and is responsible for the next 10 per cent of losses; Tranche 4 has a principal of $75m and is responsible for all remaining losses.

The yields in Figure 2 are the rates of interest paid to tranche holders. These rates are paid on the balance of the principal remaining in the tranches after the losses have been paid. Consider the first tranche. Initially, the 35 per cent is paid on $5m, but after the tranche has had to absorb losses of $1m, it is only paid on $4m. Tranche 1 is quite risky and, in a five-year deal, could get totally wiped out. It is normally retained by the creator of the CDO. By contrast, Tranche 4 is usually rated AAA and is unlikely to have to bear any losses.

Figure 2: **A cash CDO**



Once the structure in Figure 2 became established, market participants realised that they did not have to buy bonds to create a CDO. All they had to do was sell a portfolio of credit default swaps. The income from the swaps is distributed to tranche holders and there are rules, similar to those in Figure 2, for determining which tranches are responsible for which losses. A structure created in this way is known as a synthetic CDO.

The CDX IG and iTraxx portfolios are used to define standard CDO tranches. In the case of CDX IG, the first standard tranche, known as the equity tranche, is responsible for losses between 0 and 3 per cent. The second tranche, known as the mezzanine tranche, is responsible for losses between 3 per cent and 7 per cent. The remaining tranches are responsible for losses in the ranges 7 to 10 per cent, 10 to 15 per cent, and 15 to 30 per cent.

There is now an active market in what is known as single tranche trading. In this, the CDO is not set up by buying bonds or selling credit default swaps. One side agrees to buy protection on a tranche of a portfolio (usually one of the standard tranches of CDX IG or iTraxx). The other side agrees to sell protection. Cash flows are calculated as though a synthetic CDO had been set up.

The trading of CDOs and similar products is sometimes referred to as correlation trading because the value of a tranche is dependent on the extent to which defaults are correlated. Consider the set up in Figure 2. If there is no default correlation, defaults are spread fairly evenly through time. In this case, Tranche 1 is very risky since there will likely be a few defaults in a five-year period, but it is highly unlikely that Tranches 3 and 4 will have to absorb any losses. As default correlation increases, defaults tend to come in clusters. In this case, Tranches 3 and 4 become more risky, but paradoxically, Tranche 1 becomes less risky.

There is no shortage of creativity in this market. A product known as a CDO squared – formed from a portfolio of CDO tranches – now trades actively. Some banks have even traded CDO cubeds (formed from a portfolio of CDO squareds). It is now possible to find a market for deals where the payoff is any complicated function of the losses from multiple portfolios.

There is a certain irony in all this. When they created a market for credit derivatives, banks gave themselves a way of managing their credit risks. However, the products that they trade have now become so complicated that the management of credit risks is more challenging than ever before.

John Hull and Alan White are professors of finance at the Joseph L. Rotman School of Management, University of Toronto. Their research interests are in the areas of derivatives pricing and risk management.
hull@rotman.utoronto.ca
awhite@rotman.utoronto.ca