LOSING CONTROL

By Mark Eardley, SuperVision Biometric Systems.

Mark Eardley.

Evolving corporate cybercrime and escalating losses points to a loss of control in IT security.

Regulatory compliance has compelled many organisations to consider and counter the risks of having customer data stolen. But compliance in this area may have created a dangerous blind spot when it comes to recognising the more damaging consequences caused by the cyber theft of corporate secrets.

Theft of custodial data, such as the 100 million customer records stolen from Sony in May 2011, attracts far more attention than the theft of intellectual capital or secrets. It's highly newsworthy because it potentially affects so many individuals whose data has been stolen and who may be vulnerable to identity-based fraud.

But this heightened awareness perhaps creates even more pressure to protect custodial data, shifting the focus even further away from protecting secrets.

Corporate secrets are now the jackpot

Commenting in June on the findings of Verizon's 2011 Data Breach Investigations Report, (DBIR) Dave Ostertag, global investigations manager at Verizon Business, said, "I think what we're seeing is that there's a big change in the type of data that criminals are going after.

"There's a glut of personal data out there now and there really isn't a great market for it. The value of intellectual property, on the other hand, is much higher. Criminals are finding that they can make as much money from stealing a smaller number of highly sensitive records as they can from stealing a big database of customer information."

Ostertag's comments carry significant authority: now in its seventh year, the DBIR's findings are based on investigations into over 1700 data breaches and the report is probably the world's leading examination of corporate cybercrime. The last two reports have combined research into cybercrimes by both Verizon and the US Secret Service – an agency tasked with protecting America's financial infrastructure and payment systems as well as guarding the president.

This message about the changing focus of cybercrime was reinforced in February this year by a UK government report which estimated that the cyber theft of corporate secrets cost UK companies £16.8 billion to R185 billion – and accounted for almost 60% of all the country's cybercrime losses in 2010. The UK report shows that losses from the cyber theft of secrets are over four times higher than the £4 billion lost to high-profile cybercrimes involving identity theft, online fraud and theft of customer data.

The growing threat to corporate secrets was also highlighted by a March 2011 report from McAfee, which stated that, "While it remains a profitable enterprise to buy and sell stolen credit cards, lately, intellectual capital has become the new source of large and easy pay-outs."

And there's plenty of evidence to illustrate the realities of the cyber threat to intellectual assets. During 2009 and 2010, the corporate secrets of hundreds of organisations were the focus for two sets of serial cyber attacks now known as Operation Aurora and Night Dragon. High profile corporate targets of Aurora included Google, Northrop Grumman, Morgan Stanley, Dow Chemical, Yahoo and Adobe. McAfee's report says that the Night Dragon series of cyber attacks were specifically focused on stealing secrets from oil and gas companies around the world and that highly sensitive information including project financing and bidding documents was stolen over a period of several months.

Knowledge is financial value

Intellectual assets such as those that can be patented or similarly protected represent only part of the information that organisations need to hold securely. The overall knowledge base of confidential information is multi-faceted and might include production processes, R&D findings, source code, formulae, M&A activity, partnerships and alliances, product rollouts, financing arrangements, contract bids and deal negotiations, pricing structures, legal activities, financial forecasts and results, and strategic plans.

From a South African perspective, the UK government report on cybercrime says that mining companies headquartered in the UK lost £1.6 billion – some R18 billion – through the cyber theft of corporate secrets in 2010.

The report suggests that this was due to the "increasing market value of raw minerals and the high level of mergers in this sector at present." It also suggests that

mining companies are particularly vulnerable to the theft of corporate information as opposed to operational information. The difference perhaps being not how you dig, but where you are planning to dig and who is going to be digging with you.

Creating huge vulnerabilities

The abuse of traditional IT access credentials like cards, PINs and passwords lies at the heart of most corporate cybercrime – even the most sophisticated ones.

"...abuse of traditional access credentials lies at the heart of cybercrime."

The term advanced persistent threat, or APT, is increasingly used to categorise cyber theft that is sophisticated, organised and determined. The other defining characteristic of an APT is its specific purpose: stealing corporate secrets.

A March 2011 analysis by IBM of cybercrime trends and risks says that a common denominator within APTs is "that the attacker attempts to use legitimate protocols and masquerade as a legitimate user whenever possible."

In 2010, Ernst & Young and Deloitte both published commentaries on the increasing cyber threat to corporate secrets posed by APTs and emphasised the vulnerabilities created by traditional credentials. Deloitte said: "In many cases, cyber criminals have obtained credentials and accessed systems as if they were actual employees and customers. Thus, the integrity of the endpoint that is being granted access to the organisation's systems and data must be a primary concern.

"Authorised users can access and travel throughout a system, remove or change data in the system, and conduct transactions. When cyber criminals employ such users as unwitting accomplices ... they can operate as if they were users. They can acquire the same, or even greater ability to navigate pathways, copy data, execute transactions and monitor keystrokes."

Ernst and Young's comments support this opinion concerning the risks exposed by conventional IT access credentials: "A common characteristic of APT malware is that it seeks to steal the credentials of valid users so that it can execute as a legitimate user and better evade detection."

These vulnerabilities were also highlighted by Verizon's 2010 DBIR, which says: "The use of stolen access credentials was the number one hacking type in the data breaches that were investigated by Verizon and the Secret Service. It might be hard to believe, but stolen IT access credentials were the commonest way attackers gained access to enterprise systems."

But the credentials were rarely stolen using methods such as key logging, social engineering or phishing. According to Bryan Sartin, Verizon's director of investigative response, "Most of what we saw was simple exploitation of guessable passwords. These were not very sophisticated hacks at all.

"Stolen credentials offer an attacker many advantages, not the least of which is the ability to disguise himself as a legitimate user. Authenticated activity is much less likely to trigger IDS (intrusion detection systems) alerts or be noticed by other detection mechanisms."

We all know that cards, PINs and passwords are all routinely lost, forgotten and shared. Even American presidents have mislaid their 'biscuit', a card that holds numbers which open a briefcase – known as the 'football' – containing US nuclear launch codes. Bill Clinton apparently lost his for several weeks and Jimmy Carter is said to have sent his to be dry cleaned with a suit.

The advent of so-called strong passwords, smartcards and one-time PINs does nothing to alter the fact that anyone can use your credentials and you can use theirs. They are inherently insecure. Even the security of EMV compliant Chip & PIN payment cards has been shown to be fundamentally flawed and was demonstrated to be so by a Cambridge research team on BBC's Newsnight in 2010.

IT access credentials are now a target

Aside from being repeatedly lost, shared and forgotten, IT access credentials are increasingly being stolen. Bryan Sartin, director of investigative response at Verizon, said in April this year that with prices reaching $30 000 per account, usernames and passwords are the most common type of records traded on the cyber black market and have the highest per-record value.

The realities of Sartin's comments were exemplified by a recent cyber theft at RSA. In March 2011, RSA announced that cyber villains had stolen secrets about SecurID, a two-factor authentication product based on static and one-time PINs that manages IT access for some 40 million employees at over 30 000 companies worldwide.

If not immediately obvious, the reasons why cyber villains would want to steal secrets about SecurID became clear a few months later. The incident at RSA appears to have led directly to an attempted cyber theft at Lockheed Martin in May.

Describing this attack as "significant and tenacious", Lockheed said it would be replacing its SecurID tokens and was instructing all employees to change their passwords. As the world's largest defence contractor, it is obvious that Lockheed wasn't targeted for its custodial data.

The cyber theft at RSA was based on the exploitation of employees' access credentials. RSA says that the cyber theft began with a spear phishing attack on targeted employees that led to one of them opening a malware-loaded Excel file entitled '2011Recruitment plan xls'. The malware opened a backdoor on the target's computer, enabling the villains to control it remotely. Using the target's access rights, the villains then climbed RSA's internal authorisations ladder, stealing more credentials and increasing the privileges associated with them in user, domain admin and service accounts.

It seems that RSA employees were not using SecurID to authorise themselves within their own systems and that usernames and passwords were yet again at the very heart of yet another collapse in IT security.

The Aurora thefts were executed in much the same way as the theft at RSA. Earlier this year, Heather Adkins, Google's information security manager, said their exposure to Aurora started with a spear phishing campaign targeting a small number of employees.

Just as in RSA's case, information on these targets was apparently gathered from social media networks. Spear mails sent to the targets were designed to motivate visits to a photo Website set up by the people behind Aurora. One of the Google targets clicked on a link to the Website, triggering the backdoor process and subsequent credential exploitations within Google's IT systems.

Mega losses in the real world

The damage caused to RSA by the cyber theft of its secrets is known to be substantial. Several of their competitors have offered to replace SecurID products with their own security solutions. For example, within days of RSA's announcing the cyber theft, Computer Associates said it would step into the breach and swap SecurID tokens with its own IT authentication product – for free – and throw in a three-year enterprise licence.

Following the attempted cyber theft at Lockheed, RSA announced their own free replacement programme for SecurID tokens. In a Reuter's interview at the end of June, the company said that in order to implement this programme it intended to increase production of SecurID tokens into millions per month from a baseline of a few hundred thousand.

This was in addition to mounting a massive customer outreach initiative in April that involved supplying over 60 000 customers with security info and advice; making 15 000 customer phone calls; conducting conference calls with another 5 000 of them and holding hundreds of face-to-face meetings. And in July 2011, RSA announced that it was allocating $66 million (R462 million) to fund their response to the theft – a figure that excludes costs arising from possible legal actions against them and the company's inevitable loss of customers and credibility.

In response to the world's largest theft of custodial data, Sony has said it is spending $171 million – R1.2 billion – in remedial activities such as increasing IT security and providing identity protection and apology freebies to its customer base.

To put that $171 million into perspective and to illustrate the changing nature of crime, it is worth noting that in 2005, a Brazilian bank experienced one of the biggest cash robberies of all time – about $70 million in used banknotes went missing down a tunnel dug into the vault. The cyber theft at Sony will cost the company at least $100 million more than that old-fashioned heist. And even though Sony's R1.2 billion is a massive allocation it apparently does not include costs for any customer-based legal actions against them or fines that may be imposed for inadequate data protection.

Cyber villains are smart villains

For American bank, Citigroup, the May 2011 cyber theft of details on over 360 000 card holders led to the company issuing over 217 000 new credit cards at the beginning of June as well as reinforcing its IT security and account monitoring measures. But the reinforcements at Citigroup have not been entirely successful. The bank disclosed at the end of June that some $2.7 million had already been lost to fraudulent payments on over 3400 of the affected cards.

An yet when it first announced the cyber theft, Citigroup said that the stolen data was insufficient to enable transactions – customers were not at risk since Social Security numbers, birth dates, card security codes and expiry dates were not taken. It now seems that card numbers, addresses, holders' names and e-mail details were an effective starting point for the cyber villains and that $2.7 million is sufficient incentive to leverage such limited data.

The message here is clear: give the cyber villains an inch and they will take a mile.

A June 2011 report by Cisco Systems on the evolving nature of cybercrime says that the volume of spray-and-pray malicious spam has declined by more than half in the past year. At the same time, highly personalised, focused e-mail based attacks have tripled because they offer far better ROI to the cyber villains.

The report divides these focused e-mail campaigns into two categories: spear phishing and targeted attacks. Spear phishing covers activities that are aimed at groups of potential victims who share a common feature – for example, corporate customers of a specific bank.

Cisco estimates a spear phishing attack costs five times that of a mass attack. The villains' investment might include list acquisition, leasing a botnet, e-mail generation tools, malware purchases, Website creation, campaign administration tools, order processing and fulfilment infrastructure, and background research on targets.

The report says that the return on such an investment for a single spear phishing campaign can be more than 10 times that of a mass attack.

The content and format of both spear phishing e-mails and of the Websites to which they commonly direct victims are often sufficiently convincing in their attempt to establish legitimacy. In an attack on a group of banking customers, the typical objective will be to deceive victims into supplying usernames and passwords, enabling illicit transactions on the victim's account.

Focusing on much lower numbers of victims, Cisco defines targeted attacks as being "directed at a specific user or group of users, typically for intellectual property theft". The report says: "Targeted attackers often build a dossier of sorts on intended victims, gleaning information from social networks, press releases, and public company correspondence."

Allied to highly targeted spear e-mails, Cisco says these attacks, "generally employ some form of malware in order to gain initial entry to the system and to harvest desired data over a period of time."

Governance alarm bells?

At the highest executive level, the losses caused by cybercrime should certainly serve to highlight the routinely damaging consequences of lax IT security. What should add to alarm in the boardroom is the fact that, typically, the Sony and Citigroup breaches both appear to have been based on elementary exploits – an underlying feature of most corporate cybercrime.

Perhaps we need to recognise that data governance – statutory or not – should be receiving the same diligence as, say, corporate brand management and financial reporting. Speaking at the launch of the UK government's cybercrime study in February this year, the then minister for security said that many companies do not know what the normal functioning of their IT systems looks like because they don't actually know enough about their own systems. In other words, organisations are not doing enough to protect themselves from the cyber threat and the villains are running rings round IT security.

Protecting sensitive data means winning back far more control over who can access that data. The evidence is overwhelming that the status quo in user authentication just isn't working. If cards, PINs and passwords are no longer an effective barrier to the cyber-theft of secrets, is it perhaps time for us to break our reliance on them?

For more information contact Supervision Biometric Systems, +27 (0)82 463 3060, www.supervision.co.za

This article has been shortened. The full version can be found on www.securitysa.com.