G4S launches new foam shield to protect CIT

Criminals' lives just got a little tougher, thanks to G4S Cash Solutions SA. In April, the cash transporting specialists launched the Penman Foam Protection System for cash-in-transit vehicles, with a live demonstration for stakeholders and media at Bulugaya Engineering in Randburg.

This radical new foam system is an almost fail-safe deterrent and reduces reliance on security guards, thereby minimising the capacity for human error. It relies on innovative technology to protect valuable cash assets.

More than 40 vehicles will be equipped with the Denial of Access (DOA) system, which can trigger rapidly expanding foam, which hardens into a rubber barrier between the criminals and the cash.

From flash to bang, the system takes less than a minute to take effect. When triggered, two chemicals are forced from a high pressure from cylinders. The liquids combine and, in seconds, turn to foam which fills the vehicle's vault almost like a bubble bath, or a cake left in the oven too long.

Once hardened, the material cannot be melted with chemicals or fire. It would take a criminal a long time to chip away at it, by which time the criminal will have fled or the police and other security personnel will have arrived at the scene.

Hannes Venter

The directors take great pride in the new system. G4S is a leading international security solutions group. It specialises in outsourced business processes in sectors where security and safety risks are considered a strategic threat.

Representatives from G4S's top clients – including the Reserve Bank, ABSA and Western Union – were at the gala launch of the latest product at Bulugaya Engineering, which manufactures G4S vehicles.

The DOA system will be used in vehicles that move from safe location to safe location, especially those transporting bulk currency and precious metals.

"The system has been successfully piloted in other countries in Europe and the United Kingdom, and has been tailored for the South African environment," says **Hannes Venter**, G4S sales director. "The system is fully integrated with the vehicle's tracking and door-locking system. It can be triggered by a panic button held by the driver; or remotely by an operator at our national control centre."

Furthermore, the system will also be triggered if an unauthorised person tries to tamper with the doors of the vault before the vehicle arrives at its correct destination.

In the last few years, the number of violent CIT heists has decreased, largely due to the kind of deterrents the DOA system represents. While there is still a vulnerable risk element of cross-pavement snatching, Mr Venter believes the use of the foam system aligns with G4S philosophy of finding ways to keep staff safe. G4S is committed to keep safeguarding the lives of security officers and members of the public. The use of foam eliminates the need for an armed security guard in the vault.

"Rather than relying on lots of people with guns to protect our vehicles, we are using the latest technology to deter and deflect criminals," he concluded. "This approach is optimal both from a public safety perspective, as well as from the point of view of keeping our clients' cash and valuables safe." ■

SA business at risk from international hackers

THE criminal's battleground is now the virtual world, and South African businesses are at risk from these shadowy hackers and opportunistic criminals.

At a recent BECSA function in Johannesburg, **Henry Peens,** of Yelloworx IT Security Solutions, spoke about the cyber security threat landscape.

As part of on-going advocacy, Business Espionage Counter-Intelligence South Africa (BECSA) promotes business counter-intelligence in South Africa. Chairman **Steve Whitehead** believes it is poised to become an authoritative voice on the subject.

"We provide protocols, controls and guidelines to help business owners counter the growing threat of business espionage," he says. "We want to be the COSATU of counter-intelligence in South Africa."

Similarly, Yelloworx IT Security Solutions aims to equip businesses with the strategies to stop enemies gaining access to their systems. A sophisticated malware attack can track specific information for many reasons: financial gain, extortion, to bring down a small business or entire government. Technology is just another way for criminals to steal, and no system is secure.

IF YOU'RE ONLINE, YOU'RE AT RISK

With field experience in government and private intel, Mr Peens is a specialist in security and counter-intelligence in South Africa.

"Often companies buy security solutions that get shelved, or are used 10 per cent of the time," he remarks. "Security is essentially a leadership problem. Management needs to take ownership of it and buy into a strategy."

There is a gap in South African legislation covering economic espionage and, while there are white papers being developed, businesses need to empower themselves with knowledge about cyber crimes.

"The bottom line is that the threat of theft for businesses is real," says Mr Whitehead. "It has shifted to the cyber environment. The virtual world is the new battleground. The underground world of cyber crime is a billion dollar business; bigger than even the drug trade." For example: the Eurograbber Trojan virus stole €36-million in just 30 days across Italy, Spain and Germany.

In 2013, smarter technology has us connecting to the Internet through not only the PC, but via iPads, Android devices, and smartphones. Social media (Facebook, Linked-In, Twitter) have also increased how much information we share with others. In the last few years, we have also seen widespread Cloud adoption to store information. This is where the danger lies for us, and where opportunity arises for cyber criminals.

RISK INCREASES WITH CONNECTIVITY

"Criminals have more opportunity to access your information through these devices, sites

and applications," Mr Peens points out. The greater the connectivity, the greater the risk. For example, when Egypt built greater IT infrastructure, it saw an overwhelming 280 per cent spike in cyber crime. It wasn't prepared for the attack wave.

Who is behind these attacks? "Cyber criminals top the list – hackers in it for the money, especially from North Korea, Syria and the DRC," he explains.

Moreover, India and Pakistan, where there are high levels of skills and high levels of poverty, are breeding grounds for hackers. Chinese underground organisations are also supporting and assisting cyber criminals to gain a foothold in Africa, because it doesn't have proper legislation or online security – and that includes South Africa.

"However, there are also hacktivists, who hack for a political or social cause," he adds. "In fact, recently Woolworths and the University of the Free State both fell victim to this type of hacktivism. Woolworths account holder information was posted online and more than 700 000 student records were compromised."

However, typical hackers steal resources and information, or set to extort money or destroy reputations. And no one is safe, it seems. Bigger enterprises are the focus of targeted attacks, data breaches and end-user disruption. Pricing information, marketing strategies and intellectual property can be surreptitiously stolen and given to competitors.

Governments can be the target of cyber sabotage by political enemies or rogue activists, in the case of the Wikileaks debacle and the cult figure of **Julian Assange**. Even the fourth estate is not immune, he adds. The *New York Times* and *Wall Street Journal* were also the victims of recent cyber spying.

DEATH, TAXES AND ID THEFT

"However, small businesses are the most vulnerable and can also be victimised," Mr Peens says. "Their bank accounts can be hacked, or their business systems disrupted. Recently, a Johannesburg primary school's records were stolen and held to ransom."

For an end-user, the ordinary Joe Soap, there are three things he can be assured of: death, taxes, and identity theft. "Criminals use SMS and e-mails to commit identity theft," Mr Peens says. Individuals are also scammed for money.

"Our mobility and reliance on our own devices such as tablets and cellphones have put us at risk," he adds. "The mobile explosion is a major issue. It is linked to a malware explosion with virus writers targeting mobile devices, which don't have the anti-virus software PCs and laptops have. You won't even be aware of them – until it's too late."

In this regard, Apple seems to offer the most protection to users, he adds, while BlackBerry and Android devices lag behind.

ATTACK/KILL CHAIN

Cyber criminals use an advanced persistent threat (APT) process, which includes reconnaissance and weaponisation before the delivery of an attack through malware – eg botnets, zombies, trojans. Once they have broken in, they exploit or take control of systems before exfiltration. "They get out before you even know they were there," he says. "The attacks are carefully co-ordinated and executed using the most sophisticated methods."

While the growth number of PC users has remained stabled, in the last two years we have seen a worldwide explosion of smartphone and tablet users – from 300-million smartphones in 2011 to a staggering 819-million in 2013; from 15-million tablet users to 116-million in the same period.

"The problem is there is no corporate control or even policies for PCs, phones, and tablets," Mr Peens says. "From a memory stick to clicking on a link in an e-mail, or even an app on a phone, there can be serious security breaches."

There are no serious repercussions for these criminals in South Africa because of poor legislation and vaguely defined statutes. This explains why South Africa is one of the biggest spam-receiving countries in the world. Wide open for attack, we have become the target of cyber criminals from China, Russia and as far afield as Albania. Syndicates use the most sophisticated methods and blended attacks to extort individuals and businesses, and to steal money and other sensitive information.

LEGAL AND HR ISSUES

Once a spy or cyber criminal has executive command of a cellphone, he can use GPS tracking to follow an individual, access to a diary or personal appointments. A voice recorder can be unobtrusively triggered to record a board meeting. The same can be done on the webcam on a PC. Similarly, key loggers can copy key strokes and learn passwords. This can all be done by one man sitting in a room thousands of miles away.

"There needs to be greater security awareness around mobile devices," he stresses. "Not only does it need to be outlined in personal and company contracts, it needs to be entrenched in legal and human resource policy too."

Continued on page 12

Did you know?

- Two out of three adults use mobile devices to access the Internet.
- 36 per cent of Facebook users have accepted friend requests from people they did not know.
- Three out of 10 users received posts and messages from people that are not actually friends.

BECSA abroad

BECSA is organising a special tour to the US for those responsible for the protection of information in their organisation.

Counter-intelligence practitioners, TSCM specialists, security professionals and those managing these functions will benefit from taking part in this tour from 16-28 September 2013. For more information, visit www.becsa.co.za.

Arun Green ...
doyen of the South African safe manufacturing industry

By Godfrey King, Publisher, Security Focus

One of life's perfect gentlemen is how I have always viewed **Arun Green**, doyen of the South African safe manufacturing industry, who died on 12 April 2013, after a long illness.

Arun Green ... always smiling.

Arun had been in the security industry for more than 50 years, during which time he built Mutual Safe & Security into the largest family-owned local safe company.

Arun had a most affable personality, and I never saw him when he wasn't smiling.

Perhaps the most striking role he played was along with his wife **Carol**, as together they formed a leadership team which had a certain "style". We featured them on our cover in September 1997 under the title "Married to the safe business".

Carol was only the second female to be featured on our cover and I described her in an editorial as "one of the sexiest security directors in the industry".

While Carol has since retired, both their sons are still in the family business. The younger son **Jason** holds the position of as chief executive officer in South Africa, and elder son **Rowan** heads up Mutual's arm in the United States.

Like many people in the early years of the South African security industry, Arun had an East African background.

He was born in Mombasa, Kenya, in 1944. After the war, his parents – his father was in the RAF and his mother in the WAF – decided to take their demobilisation packages from the British government and move to South Africa.

After leaving school, Arun joined Chubb in 1961 as an apprentice locksmith, where he rose up through the ranks to the position of sales manager, leaving in 1974 to buy 50 per cent of the Pretoria-based Bischoff Safe Company. In 1978, he sold the company to Murray & Roberts, who shortly afterwards acquired Giant Security as well. After further acquisitions, the Bischoff Electro Group was established.

In 1984, Arun moved out on his own and, with two colleagues, founded Mutual in a very small factory in Rosslyn, Pretoria. The rest, as they say is history.

Along the way, Mutual took over Austen, arguably the best known trade name for safes in South Africa. It is also the oldest safe manufacturer in the country. ■

SA business at risk from international hackers

Continued from page 7

DARK CLOUDS ON THE HORIZON

Cloud and virtualisation is the next big thing in the cyber threat landscape. There are growing security risks in storing information this way, Mr Peens believes. This information can be compromised by insecure data deletion, or even malicious insiders.

"Recently, there was controversy around SSL Certificate Authentication not being verified properly," he says. "There were so many applications that some were passed without the proper compliance."

While South African cyber law is evolving, individuals and businesses need to become more aware of potential security breaches – from the tea person to the chief executive officer. "The more we talk about it, the better," Mr Peens says. "Make sure you have all the resources available to keep yourself safe from these types of cyber attacks."

In order to make BECSA more effective and push for better legislation in counter-intelligence, **Steve Whitehead** wants to grow its membership. "To do this, we need sponsorship and more members," he concluded. "We want to help our members grow their business, become more tech savvy and see us as a repository of key information and support." ■