Organised cyber criminals are digital mafia

In the wake of the Tesco Bank hack, which saw 9,000 customer accounts targeted, cyber security experts are warning of organised online crime gangs operating like a digital mafia.

Either way you look at it, says Adrian Nish, who leads the Cyber Intelligence team at IBM Security’s cyber defence division. ‘Resilient hackers are as good as or even better than armies. It’s a different mindset. A lot of high-profile attacks result from well-known hackers. Many use freely available software, as in the recent TalkTalk hack,” he says. “But they have a motive.”

The new breed of cyber criminals see themselves as digital mafiosos. The malvolent hackers behind the DrinkSmashRecycle scam, for example, made off with 183,000 credit card account numbers. The hackers then sold them on the Darknet for $13 per account.

Cyber criminals are also a challenge, but to old-school hackers is a challenge, but to teenagers looking for money. “What makes them different from old-school hackers is that they have a market,” he says.

This new breed of cyber criminals see themselves as digital mafiosos. The Maldev hackers behind the DrinkSmashRecycle scam targeted victims by e-mailing a fake email from a company called SecureBank, and used contact form to lure people into giving their personal information.

Although this publication is funded through advertising and sponsorship, all editorial is without bias and anonymous and are not influenced by our advertisers. To contact us please e-mail info@raconteur.net or call 44 (0)20 8616 7400

Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. raconteur.net is now a writer for The Guardian and The Register. For contributions and speaking engagements, please get in touch.

© Raconteur Media
All rights reserved. Produced by Lloyds Banking Group
raconteur.net

Share this article online via raconteur.net

 raconteur.net

 raconteur.net
Tens of thousands of connected devices are now connected to the internet, raising major security concerns.

Mr Manky, who explains that most businesses are not seriously engaged in protecting against a cyber threat, says this is a significant issue for the coming years.

Mr Manky makes clear that the number of vulnerabilities in systems is increasing and that the need to integrate the network and security infrastructure in a more comprehensive way is critical.

Mr Manky says that enterprises are falling short of the necessary investments in cyber security.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky believes that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manky says that enterprises are not adequately resourced in terms of security, but that they need to do so in order to ensure the underlying network infrastructure is secure.

Mr Manka...
Beware the home appliances that can attack

The internet of things, connecting devices and collecting data, holds great promise for business, but presents a serious cybersecurity risk.

The rise of machines is upon us, and the cost of internet-connected devices years on from now may dwarf what is already possible. For both business-

vulnerabilities in the device themselves could be used to compromise the targeted device. Hackers might be able to use this kind of attack on, say, an exposed, public-facing home network, or a vulnerable home network’s part of a larger network of a business. This is not as complicated as hacking into devices still running Linux open source operating system.

The scale of the attack has caught the attention of politicians. Chancellor Philip Hammond referred to attacks that take advantage of the Internet of Things (IoT) security problem.

Government needs to make laws and en forces them, he says. “Every day, we are learning something new. We must ensure that government may have a role to play in making these laws.”

Takashi Shiraishi, senior research manager at Rapid7, says Shodan, the search engine for the Internet of Things, makes it easy for hackers to find machines of automating the process of hacking into devices still running Linux open source operating system.

Government needs to make laws and enforce them, he says. “Every day, we are learning something new. We must ensure that government may have a role to play in making these laws.”

Takashi Shiraishi, senior research manager at Rapid7, says Shodan, the search engine for the Internet of Things, makes it easy for hackers to find machines that are open internet with port-forwarding, translation) and firewall protections. A one-day meeting convened by the European Commission in April recommended new recommendations to other businesses about managing and securing connected devices.

A group called New World Hackers, earlier this year, suddenly launched a wave of attacks on October 21. The malware of automating the process of hacking into devices still running Linux open source operating system.

The Center for Internet and Technology Addiction (CITA) warned that 90% of consumers who buy IoT products do not set up a simple reverse shell to build management access to any device.

A director at UK security consultancy Net Test Partners, says that this rise of vulnerability is applicable to businesses in long and going. These include CCTV recording systems, computers in an organization, the network, building alarms that can be locked out. But there is also increasing demand for information security, as well as vulnerability smart coffee makers, thermostats, building management systems and more.

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?

None of them are vulnerable to IoT-related risk?

WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?
Cyber security is making a noise

Top state-sponsored attacks have triggered an international cyber arms race aimed at repelling and even retaliating if secrets are stolen or online infrastructure targeted, threatening to paralyse critical systems.

The US and Russia are the main culprits, and that this move has been continued into the cyber age should surprise nobody.

The US Department of Homeland Security is using state-sponsored cyber attacks as a tool to disrupt the functioning of critical infrastructure, the agency’s head said.

That said, while there can be little doubt some nation states are far more advanced than others, it doesn’t take a cyber threat to wake up the US government. It has already been done.

‘Silent’ cyber arms race is making a noise

Suspicious state-sponsored attacks have triggered an international cyber arms race aimed at repelling and even retaliating if secrets are stolen or online infrastructure targeted, threatening to paralyse critical systems.

The US and Russia are the main culprits, and that this move has been continued into the cyber age should surprise nobody.

The US Department of Homeland Security is using state-sponsored cyber attacks as a tool to disrupt the functioning of critical infrastructure, the agency’s head said.

That said, while there can be little doubt some nation states are far more advanced than others, it doesn’t take a cyber threat to wake up the US government. It has already been done.

As sophisticated cyber criminals become increasingly aggressive and collaborate with offline criminals, banks face a greater threat than ever before. However, one simple innovation could improve their security significantly.

They have knowledge of the online world who are receiving fake salaries, but this doesn’t mean they understand how banks work.

Mr Slavin said at Kaspersky Lab.

They’re also seeing a blend of online and offline fraud, he said.

Slavin, UK and Ireland general manager at Kaspersky Lab.

As sophisticated cyber criminals become increasingly aggressive and collaborate with offline criminals, banks face a greater threat than ever before. However, one simple innovation could improve their security significantly.

They have knowledge of the online world who are receiving fake salaries, but this doesn’t mean they understand how banks work.

Mr Slavin said at Kaspersky Lab.

They’re also seeing a blend of online and offline fraud, he said.

Slavin, UK and Ireland general manager at Kaspersky Lab.

As sophisticated cyber criminals become increasingly aggressive and collaborate with offline criminals, banks face a greater threat than ever before. However, one simple innovation could improve their security significantly.

They have knowledge of the online world who are receiving fake salaries, but this doesn’t mean they understand how banks work.

Mr Slavin said at Kaspersky Lab.

They’re also seeing a blend of online and offline fraud, he said.

Slavin, UK and Ireland general manager at Kaspersky Lab.

As sophisticated cyber criminals become increasingly aggressive and collaborate with offline criminals, banks face a greater threat than ever before. However, one simple innovation could improve their security significantly.

They have knowledge of the online world who are receiving fake salaries, but this doesn’t mean they understand how banks work.

Mr Slavin said at Kaspersky Lab.

They’re also seeing a blend of online and offline fraud, he said.

Slavin, UK and Ireland general manager at Kaspersky Lab.

As sophisticated cyber criminals become increasingly aggressive and collaborate with offline criminals, banks face a greater threat than ever before. However, one simple innovation could improve their security significantly.

They have knowledge of the online world who are receiving fake salaries, but this doesn’t mean they understand how banks work.

Mr Slavin said at Kaspersky Lab.

They’re also seeing a blend of online and offline fraud, he said.

Slavin, UK and Ireland general manager at Kaspersky Lab.

As sophisticated cyber criminals become increasingly aggressive and collaborate with offline criminals, banks face a greater threat than ever before. However, one simple innovation could improve their security significantly.

They have knowledge of the online world who are receiving fake salaries, but this doesn’t mean they understand how banks work.

Mr Slavin said at Kaspersky Lab.

They’re also seeing a blend of online and offline fraud, he said.

Slavin, UK and Ireland general manager at Kaspersky Lab.

As sophisticated cyber criminals become increasingly aggressive and collaborate with offline criminals, banks face a greater threat than ever before. However, one simple innovation could improve their security significantly.

They have knowledge of the online world who are receiving fake salaries, but this doesn’t mean they understand how banks work.

Mr Slavin said at Kaspersky Lab.

They’re also seeing a blend of online and offline fraud, he said.

Slavin, UK and Ireland general manager at Kaspersky Lab.

As sophisticated cyber criminals become increasingly aggressive and collaborate with offline criminals, banks face a greater threat than ever before. However, one simple innovation could improve their security significantly.

They have knowledge of the online world who are receiving fake salaries, but this doesn’t mean they understand how banks work.

Mr Slavin said at Kaspersky Lab.

They’re also seeing a blend of online and offline fraud, he said.

Slavin, UK and Ireland general manager at Kaspersky Lab.
The United States has more capacity than anybody, both offensively and defensively, when it comes to cyber weaponry.

What there isn’t, nor would you expect there to be, is an increased budget for cyber warfare. But, at least so far, the US has been more cautious than the United Kingdom in publicising its decisions about the Defence Review, even if there are reports about the existence of a Cyber Command.

Is it possible for the United States to retain its pre-eminence in the cyber domain? That is, says Mr Couch “leveraging what we know about breaking in to others to defend in the future.”

That is, says Mr Couch “leveraging what we know about breaking in to others to defend in the future.”

That raises a question about how much emphasis is being put on the development of cyber arms. FireEye has estimated that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

It’s not, after all, just about attacking with cyber weaponry. “Traditionally, almost all cyber investment figures that are suggested are based on 2012, when it comes to defence in the blind.” In other words, everyone focused on defensive capability, and anyway the ability to inflict the most damage is not as simple as who invests the most money. It’s not whether one is highly motivated and equipped with the right tools and access, but whether the investment figures that are suggested are based on the openness of former intelligence. Equally a highly funded, well-organised effort can achieve far greater damage than can be achieved by poorly funded, poorly motivated efforts.

So how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

That raises the question of how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

It’s not, after all, just about attacking with cyber weaponry. “Traditionally, almost all cyber investment figures that are suggested are based on 2012, when it comes to defence in the blind.” In other words, everyone focused on defensive capability, and anyway the ability to inflict the most damage is not as simple as who invests the most money. It’s not whether one is highly motivated and equipped with the right tools and access, but whether the investment figures that are suggested are based on the openness of former intelligence. Equally a highly funded, well-organised effort can achieve far greater damage than can be achieved by poorly funded, poorly motivated efforts.

So how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

It’s not, after all, just about attacking with cyber weaponry. “Traditionally, almost all cyber investment figures that are suggested are based on 2012, when it comes to defence in the blind.” In other words, everyone focused on defensive capability, and anyway the ability to inflict the most damage is not as simple as who invests the most money. It’s not whether one is highly motivated and equipped with the right tools and access, but whether the investment figures that are suggested are based on the openness of former intelligence. Equally a highly funded, well-organised effort can achieve far greater damage than can be achieved by poorly funded, poorly motivated efforts.

So how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

It’s not, after all, just about attacking with cyber weaponry. “Traditionally, almost all cyber investment figures that are suggested are based on 2012, when it comes to defence in the blind.” In other words, everyone focused on defensive capability, and anyway the ability to inflict the most damage is not as simple as who invests the most money. It’s not whether one is highly motivated and equipped with the right tools and access, but whether the investment figures that are suggested are based on the openness of former intelligence. Equally a highly funded, well-organised effort can achieve far greater damage than can be achieved by poorly funded, poorly motivated efforts.

So how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

It’s not, after all, just about attacking with cyber weaponry. “Traditionally, almost all cyber investment figures that are suggested are based on 2012, when it comes to defence in the blind.” In other words, everyone focused on defensive capability, and anyway the ability to inflict the most damage is not as simple as who invests the most money. It’s not whether one is highly motivated and equipped with the right tools and access, but whether the investment figures that are suggested are based on the openness of former intelligence. Equally a highly funded, well-organised effort can achieve far greater damage than can be achieved by poorly funded, poorly motivated efforts.

So how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

It’s not, after all, just about attacking with cyber weaponry. “Traditionally, almost all cyber investment figures that are suggested are based on 2012, when it comes to defence in the blind.” In other words, everyone focused on defensive capability, and anyway the ability to inflict the most damage is not as simple as who invests the most money. It’s not whether one is highly motivated and equipped with the right tools and access, but whether the investment figures that are suggested are based on the openness of former intelligence. Equally a highly funded, well-organised effort can achieve far greater damage than can be achieved by poorly funded, poorly motivated efforts.

So how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

It’s not, after all, just about attacking with cyber weaponry. “Traditionally, almost all cyber investment figures that are suggested are based on 2012, when it comes to defence in the blind.” In other words, everyone focused on defensive capability, and anyway the ability to inflict the most damage is not as simple as who invests the most money. It’s not whether one is highly motivated and equipped with the right tools and access, but whether the investment figures that are suggested are based on the openness of former intelligence. Equally a highly funded, well-organised effort can achieve far greater damage than can be achieved by poorly funded, poorly motivated efforts.

So how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

It’s not, after all, just about attacking with cyber weaponry. “Traditionally, almost all cyber investment figures that are suggested are based on 2012, when it comes to defence in the blind.” In other words, everyone focused on defensive capability, and anyway the ability to inflict the most damage is not as simple as who invests the most money. It’s not whether one is highly motivated and equipped with the right tools and access, but whether the investment figures that are suggested are based on the openness of former intelligence. Equally a highly funded, well-organised effort can achieve far greater damage than can be achieved by poorly funded, poorly motivated efforts.

So how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

It’s not, after all, just about attacking with cyber weaponry. “Traditionally, almost all cyber investment figures that are suggested are based on 2012, when it comes to defence in the blind.” In other words, everyone focused on defensive capability, and anyway the ability to inflict the most damage is not as simple as who invests the most money. It’s not whether one is highly motivated and equipped with the right tools and access, but whether the investment figures that are suggested are based on the openness of former intelligence. Equally a highly funded, well-organised effort can achieve far greater damage than can be achieved by poorly funded, poorly motivated efforts.

So how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.

It’s not, after all, just about attacking with cyber weaponry. “Traditionally, almost all cyber investment figures that are suggested are based on 2012, when it comes to defence in the blind.” In other words, everyone focused on defensive capability, and anyway the ability to inflict the most damage is not as simple as who invests the most money. It’s not whether one is highly motivated and equipped with the right tools and access, but whether the investment figures that are suggested are based on the openness of former intelligence. Equally a highly funded, well-organised effort can achieve far greater damage than can be achieved by poorly funded, poorly motivated efforts.

So how much emphasis is being put on the development of cyber arms? FireEye estimates that the US military and intelligence agencies spend more than 250,000 to 300,000 staff and contractors on cyber security, and that for the first time this year, President Obama told reporters about a £1.9-billion investment in cyber, but “arms” in this domain.
What makes criminal hackers want to hack?

Cyber criminals are driven by a diverse range of aims and ambitions — so what drives them to break into a computer and steal?

**AUTHENTICATION: NEXT SECURITY FRONTIER**

Powerful new ways of verifying a tech user's identity can achieve the right balance between security and access.

**SIMPLIFY AND SECURE ACCESS TO YOUR MOBILE USERS**

- Mobile devices

**ATTACKS ON YOUR MOBILE NETWORK**

- Identity and access management

**AUTHENTICATION**

Using adaptive authentication is a way to match user verification to the potential risk of access.

**ROPHEM**

For some, cyber criminality is a career. For others, it’s a form of reimbursement. Emotet operations, spear phishing and social engineering are some of the reasons why they fall under the definition of cyber-criminal. "It’s an area of focal risk that has become more of a challenge," says Paul Purdy, a senior security consultant for Micro Focus. "Using adaptive authentication is a way to match user verification to the potential risk of access. It works by identifying the background with little impact," explains Mr Purdy.

**REVENUE**

For some, cyber criminality is a career. For others, it’s a form of reimbursement. Emotet operations, spear phishing and social engineering are some of the reasons why they fall under the definition of cyber-criminal. "It’s an area of focal risk that has become more of a challenge," says Paul Purdy, a senior security consultant for Micro Focus. "Using adaptive authentication is a way to match user verification to the potential risk of access. It works by identifying the background with little impact," explains Mr Purdy.

**BACK-END SYSTEMS**

- Access control and governance

**MOTIVATION**

Why do cyber criminals want to hack?

- Financial gain is the daddy of all motives for cyber criminal. According to Paul Purdy at Micro Focus, criminals target businesses globally in order to steal money.

**HACTIVISM**

Anarchists, Rebels, Linered Signal and Nuketrolls are some of the names of terrorist hacking groups who are primarily focused on the digital realm and are primarily target large organizations. They do their attacks to bring down a company’s computer systems, to destroy access files which can then be used for financial gain.

**SUBVERSION**

Olga Coe atSymantec points to a number of significant advances in the area of subversion, such as the CryptoWall ransomware, which is another significant group into targeted financial gain. In a report published by Symantec, it states how millions of dollars is taken, by the year 2018, this is expected to rise to billions.

**NORETORY**

Breach is a competitive sport and cyber criminals are often motivated by a sense of achievement. If you can pull off the ultimate hack of, say, a global corporate or agency, then the fame of the feat is huge.

**MONEY**

Financial gain is the daddy of all motives for cyber criminal. According to Paul Purdy at Micro Focus, criminals target businesses globally in order to steal money.

**THE CHALLENGE**

The name ‘hacker’ is ubiquitous. It doesn’t come with a value judgment attached to it, in technological or professional terms. People who fall under the definition range from ordinary people who like to exploit programs with computers to adversaries applying their skills with criminal intent.

**THE OPPORTUNITY**

It doesn’t help that the bad guys are getting way more sophisticated in their approach to attack," says Ryan Pfeifer, solutions marketing manager at Micro Focus, a multinational software and information technology company. "It’s a tech- nology war so companies on the frontline of protecting our systems need to stay one step ahead of cyber threats.

**THE OpportUNity**

It doesn’t help that the bad guys are getting way more sophisticated in their approach to attack," says Ryan Pfeifer, solutions marketing manager at Micro Focus, a multinational software and information technology company. "It’s a technology war so companies on the frontline of protecting our systems need to stay one step ahead of cyber threats.

**THE OPPORTUNITY**

It doesn’t help that the bad guys are getting way more sophisticated in their approach to attack," says Ryan Pfeifer, solutions marketing manager at Micro Focus, a multinational software and information technology company. "It’s a technolo-
Top hacker on the side of the good guys

Jamie Woodruff is an ethical hacker who helps companies keep out cyber criminals trying to break into computers to steal their money and secrets.

Jamie Woodruff

Jamie Woodruff is an ethical hacker who helps companies keep out cyber criminals trying to break into computers to steal their money and secrets.

At a young age, Woodruff had a knack for hacking, and his skills have become more refined over time. He has spent numerous years working with computers, gaining knowledge from others, and finding ways to keep computers secure. In addition to his work as an ethical hacker, Woodruff has also worked as a penetration tester, helping companies identify vulnerabilities in their systems.

Woodruff's passion for cybersecurity started at a young age. He became interested in computers when he was nine years old, and his interest only grew stronger as he grew older. He began by experimenting with his family's computer, and soon discovered that he could use his skills to help others.

Woodruff's first job was working at an old people's home before turning his attention to computing. However, it wasn't until he had the chance to begin learning more about computers and hacking that his skills began to truly shine. He soon discovered that he had a talent for working with computers, and that he could use his skills to help others.

Woodruff is a firm believer in the importance of education. He feels that it is crucial for individuals to understand the basics of cybersecurity in order to keep their information safe. He also believes that education is key to preventing cyber attacks, and that it is important for individuals and organizations to stay informed about the latest trends and threats.

Woodruff's work as an ethical hacker is an important part of the fight against cyber crime. He uses his skills to help companies identify vulnerabilities in their systems, and to develop strategies for keeping their information safe. His work is essential in the fight against cyber crime, and he is dedicated to using his skills to make the world a safer place for all.

Woodruff's work is not without its challenges. He is often called upon to work under tight deadlines, and he must be able to think quickly and creatively in order to find solutions to complex problems. However, he is up to the challenge, and he is committed to using his skills to make the world a safer place for all.

Woodruff is an example of how one person can make a difference in the world. He uses his skills to help others, and he is dedicated to using his work to make the world a safer place for all. His story is one of inspiration, and it is a reminder of the importance of education and the need for all individuals and organizations to stay informed about the latest trends and threats.

Woodruff's work is essential in the fight against cyber crime, and he is dedicated to using his skills to make the world a safer place for all.
Cyber attacks against big businesses are nothing new, with high-profile company suffering from.reductions in planned capital expenditure on security concerns. A cyber attack on a smaller organisation is unlikely to get anywhere near the level of public visibility garnered by the leaking of a multinational corporation, but this doesn’t make them any less serious. Hackers are just as likely to target small firms as they are to target larger businesses. In 2016, smaller businesses were more affected than larger ones, with over 40 per cent of small and medium-sized enterprises (SMEs) experiencing a cyber attack at some point during the year, compared to 30 per cent of larger companies. According to a report by the US National Cyber Security Division, 68 per cent of small businesses felt at least one cyber attack last year and 1 per cent were targeted multiple times.

Cyber criminals are targeting SMEs in a growing number of ways, with manoeuvrable attack vectors proving to be one of the most popular methods used to extract money. Ransomware in a type of malware that encrypts vital computer data and demands money, ransomware is a type of malware that encrypts valuable data and demands money. Ransomware is a type of malware that encrypts valuable data and demands money. Ransomware is a type of malware that encrypts valuable data and demands money.

“Unfortunately, there is still a long way to go until SMEs are as secure as they should be,” says Mr Rubin. “It is estimated that 66 per cent of cyber attacks are attempts to get into a company’s network through employee access. Cyber criminals are now using social engineering techniques to exploit this weak link in security by tricking employees into handing over sensitive information. One method hackers use is pretending to be a supplier or client to request access to the SME’s network. This can be extremely difficult for SMEs to prevent, and even harder to detect.”

In 2016, almost 80 per cent of SMEs surveyed by the Ponemon Institute said that they were vulnerable to a cyber attack, with nearly 40 per cent of these businesses suffering a cyber attack. This highlights the importance of educating staff in the best cybersecurity practices. IBM’s Security X-Force report found that employees are responsible for 60 per cent of all cyber attacks, with a quarter of all cyber incidents caused by human error. The reason for this is simple: employees are the weakest link in the security chain.

The movement towards increasing interconnectivity in businesses of all sizes can only be expected to provide new avenues for attack to be exploited by cyber criminals. A study by the US Department of Homeland Security found that 60 per cent of cyber attacks are attempts to get into a company’s network through employee access. Cyber criminals are now using social engineering techniques to exploit this weak link in security by tricking employees into handing over sensitive information. One method hackers use is pretending to be a supplier or client to request access to the SME’s network. This can be extremely difficult for SMEs to prevent, and even harder to detect.

The number of successful cyber attacks on SMEs has increased significantly in recent years, with over 40 per cent of SMEs reporting an increase in the number of attacks on their networks. This highlights the importance of educating staff in the best cybersecurity practices. IBM’s Security X-Force report found that employees are responsible for 60 per cent of all cyber attacks, with a quarter of all cyber incidents caused by human error. The reason for this is simple: employees are the weakest link in the security chain.

One thing that links SMEs to large organisations is that they are equally at risk to cyber attack - no one is immune.

The UK government has launched a 12-week consultation on the definition of an SME, with a consultation deadline of 27 November. The UK government’s plan is to define an SME as a business with fewer than 50 employees, with a turnover of less than £10 million and with an asset value of less than £2 million. This definition is designed to ensure that SMEs are able to access the support and funding they need to grow and compete.

The UK government has launched a 12-week consultation on the definition of an SME, with a consultation deadline of 27 November. The UK government’s plan is to define an SME as a business with fewer than 50 employees, with a turnover of less than £10 million and with an asset value of less than £2 million. This definition is designed to ensure that SMEs are able to access the support and funding they need to grow and compete.

The UK government has launched a 12-week consultation on the definition of an SME, with a consultation deadline of 27 November. The UK government’s plan is to define an SME as a business with fewer than 50 employees, with a turnover of less than £10 million and with an asset value of less than £2 million. This definition is designed to ensure that SMEs are able to access the support and funding they need to grow and compete.