2018

Cyber Attack Trends

Whitepaper

CHERT SECURITY


(234)
0700 2437864


enquiries
@chertsecurity.com


14, Ilaka Street Off
Coker Road,
Ilupeju Lagos,
Nigeria

Content

Executive Summary

Chert Security has responded to these security challenges by providing affordable and dynamic services that extend beyond just technology.

In this whitepaper, Chert Security have reviewed current cyber security issues affecting many areas of digital technology. From commonly used computers and enterprise servers, to IoT (Internet of Things) devices and smart automobiles, we have focused our analysis on current attack trends and the effects of intrusion on corporations. The aim of this publication is to build awareness among our readers about attack and defence trends that are currently occurring in the digital market. This report has been compiled after close collaboration between multiple departments and includes comprehensive insight from our team of security professionals. External resources include recent research papers, books, articles and guidance from academics specializing in security research and developments. By gathering information from the sources mentioned above, we have created a guide, which will aid the reader to understand the current threat landscape in the security industry.

Additionally, this report also provides an insight into Chert Security's background and how we aim to revolutionize the security industry by offering affordable and efficient security solutions to our clients.

We are committed to attaining the highest level of client satisfaction and maintaining high quality standards industry-wide.

Understanding the Threat of Cyber Attacks on Enterprise Infrastructure

Computers have revolutionized our lives since they first came into existence. From updating our digital diaries on the go to putting a man into space, to performing complex medical surgeries, digital technology is now assisting us in every aspect of our lives. Therefore, whether or not computers are an integral part of our society is no longer a question. However, this necessity of life has also attracted a lot of interest from malicious attackers, informally referred to as hackers. These hackers can be individuals or organizations who perform digital attacks to bring harm to the ordinary users, whether the users are individuals, corporations or governments. The motivation for such attacks can vary from a desire to be a nuisance, financial gain through theft or blackmail or political motivation.

Many enterprises fall victim to these attacks, which can lead to substantial financial losses, reputation damage, data breaches and subsequent lawsuits, resulting in further financial implications. A report released by McAfee in 2014 titled 'Net Losses: Estimating the Global Cost of Cyber Crime' predicted that the annual estimated losses to Global economy due to cyber crimes could be as high as $575 billion in 2015. Further analysis conducted by Forbes in 2016 concluded that the total global cost of cyber crimes could reach around $2 trillion by 2019 and could be as high as $6 trillion by 2021.

"Cyber crimes would reach around $2 trillion by 2019 and could be as high as $6 trillion by 2021."

The Nigerian Landscape

In the Nigerian economy, cyber crime amounts to 0.08 % of the Gross Domestic product (GDP). In November 2017, Internet penetration in Nigeria was hovering just over the 98.3 million people. Extraordinarily, 47.7 % of individuals surveyed reported they have experienced some kind of Internet -facilitated crime. These incidents seems to be growing, especially if unreported incidents are considered. In 2015, Information Security Society of Africa- Nigeria (ISSAN), revealed that approximately 25 % of cybercrimes in Nigeria are unresolved. Due to the huge increase in the number cyber attacks or incidents over the past two years, the percentage of unresolved incidents has also significantly increased.

The Nigerian Communications Commission (NCC) stated that Nigeria currently ranks as the worst nation for cybercrimes in Africa and third globally behind the UK and US. In 2015, the estimated loss in Nigeria was N127 billion due to cybercrime. In 2016 losses in Africa hit $2 billion, of which 27 %, $550 million, was in Nigeria. The NCC has now partnered with the US Department of Homeland Security through a cyber security awareness partnership known as "STOP.THINK. CONNECT".

The Cyber Awareness Coalition, with its unchanging commitment to end-user protection, is involved in educating the general public on the significance of cyber security. The NCC will also increasing the momentum on cyber security through October, since this month has been declared as the Cyber Security Awareness Month (NCSAM). Nigerian Communications Commission's New Media & Information Security Department has been setup to tackle new media developments and information security issues that the country is facing. The department has significant amount of media developments to handle due to the rapid growth of new media technologies and the Internet as an alternative source of Digital attacks against Small and Medium sized Enterprises (SMEs). These enterprise attacks are now so frequent that they are considered a common occurrence.

The primary reason that SME attacks becoming so common is firstly related to small enterprises under appreciating the threat of cyber security, and secondly SMEs have limited funds to implement security measures efficiently. There is an immense shortage of skilled security workers, which is making it more difficult and expensive for businesses to bolster their network against attacks. In addition, the soaring cost of security auditing solutions and security awareness training for employees, is another reason why some SMEs have not deployed effective digital defences against attackers. Chert Security has identified this serious gap in the market, and in collaboration with Cyraatek UK, Chert Security is offering affordable security solutions to SMEs.

In 2015, the Cybercrimes Act was passed into law to address these new cyber challenges. However, despite all of these measures being prioritized at a government level, the threat of digital attacks against businesses is likely to intensify. Consequently, it is becoming harder for businesses to stay on top of this threat. In addition to the number of attacks, some attackers have also devised complex techniques to stay unnoticed and unidentified once they have infiltrated an enterprise's network. A top UK insurance company Allianz Insurance, annually issues a report on the threats faced by modern world. Their 2017 report stated that cyber related incidents have increased by over 45%, making it one of the biggest threats enterprises are facing today.

The exponential growth of cloud and mobile technologies, as well as the Internet of Things (IoT) is making considerable impact on the population. Enterprises now have a diverse playing field to develop and evolve new business models. Additionally, the widespread adoption of IoT is enabling enterprises to change their branding strategies and increase their current product offering. However, continued evolution of these services has also brought unanticipated challenges for the users of these technologies.

"Fundamentally, the lack of awareness about rapidly evolving security issues is the main reason that most users and companies are failing to protect themselves from cyber attacks."

The rapid uptake of IoT devices, coupled with inadequate security mechanisms employed by these devices, this will continue to lead to substantially greater cyber security risks. The widespread consequences of security exploitation will have drastic effects, for businesses but also all technology users, from individual to Governments. The lack of awareness with regards to IoT security, among all users, is a huge concern and challenge.

Internet of Things - Threats and Challenges

Simply put, IoT is the inter-networking of physical devices (e.g. fridge, toaster, lights), which have smart features and network connectivity, that enables these devices to collect and exchange data seamlessly through the Internet. IoT is a pervasive technology which spans across many sectors.

Today, it is possible to see food cupboards within homes that can keep track of the items being consumed and then re-order the food accordingly, without human involvement. Similarly, there are products in the market like smart kettles, that can be activated remotely with a touch of a button on a mobile phone, or location aware thermostats, that can turn the heating on when they detect you are leaving office for home, and always-on voice activated virtual assistants, with the ability to carry out precise data analysis to support us in our daily lives. The recent introduction of Amazon Dash button for example, brings convenience and ease into the lives of many of their customers. Rather than a customer using their computer to reorder items, Amazon customers simply press the wireless standalone button, which then sends a 'purchase' command to Amazon, enabling the order and delivery of pre-specified item, for example an Amazon Dash button may be located in the bathroom to enable speedy reordering of toilet paper when it is running low.

Without even realizing it, we are now surrounded by IoT devices. In smart cities, IoT devices are used to manage parking, traffic congestion, street lighting and study the changing habits of the urban population. IoT sensors are being used to measure temperature inside industrial and medical storage facilities. IoT devices with diagnosis capabilities are being used in vehicles to send real time alarms to emergency services, in the case of an incident. From waste to premium food products, IoT technology is being used. The rubbish in waste management facilities is being monitored and sorted by IoT systems. Additionally, IoT devices are now even being used to enhance wine quality, by monitoring parameters including soil moisture and vineyard trunk diameter.

The reality is that the IoT industry is expanding rapidly. According to Gartner Inc., there will be 21 billion connected IoT devices by the end of 2020. Forbes reports that the number of IoT devices will reach 75.4 billion by 2025. Analysis of reports relating to this industry suggest that the exponential uptake of IoT systems has taken academics, scientists and technology sector by surprise. Devices that connect wirelessly to the Internet have now been in existence for over two decades, but it is only in the last

few years that we have observed a huge rise in their uptake, particularly within the consumer market. However, the sudden adoption of IoT in the last few years has given rise to new attack vectors.

A point to note here is the problem with IoT technology is not its rapid uptake, but the lack of security within the devices, and also the lack of security in the way that the devices connect to the Internet. Following thorough analysis of IoT devices, there is a general consensus between academics, researchers and hackers, that generally IoT devices have much weaker security features when compared to traditional computing devices.

A recent high profile security lapse was the 2017 IoT_reaper that took advantage of vulnerabilities in various IoT devices and enslaved them into a botnet network. Researchers believe that IoT_reaper malware has already infected nearly two million devices and the number is continuing to increase at an extraordinary 10,000 new devices per day. Another high profile attack in October 2016, was known as Mirai, when some of the top US Internet sites were hit by the biggest IoT-based malware. Experts describe this outage as one of the largest and most organized attacks of its kind in the Internet history. To facilitate the offensive, attackers hacked a large collection of IoT devices using a malware, known as 'Mirai', which utilized brute force and dictionary attack methods to break into poorly secured IoT devices. Once in control, the malware further infected the devices with malicious code so they could be turned into bots, which could then perform a variety of automated tasks on behalf of their masters. This huge collection of botnets was exactly what the hackers needed to launch their main attack. The botnets were used to direct massive amounts of bogus Internet traffic, approximately 990GB/s, towards the infrastructure of Dyn, an Internet performance management company and a cloud service provider. This attack caused Dyn's servers to go offline for a considerable amount of time. Consequently, companies who relied on Dyn for their services, also went off-line for the duration of the attack. Some of the well-known companies that became victims of this attack included Reddit, Paypal, Twitter and Spotify.

The danger of IoT attacks is real and can be life threatening in some cases. For example, imagine hackers taking control of the bio-medical devices embedded in humans, to assist them with their bio-functions. A hacker could then disrupt the digital mechanics of the device and intentionally or unintentionally cause damage or even death to the wearer. In February 2017 the Food and Drug Administration (USA) released a statement in which they warned that some pacemakers could be vulnerable to hacking, that under certain conditions, attackers could take control of the pacemaker, enabling hackers to deplete the battery depletion or even administer inappropriate pacing or shocks to the wearer.

"Sudden growth and adoption of IoT in the past couple of years has given rise to new attack vectors."

There have been reports in the media relating to successful unauthorized takeover by security researchers and malicious attackers, of autonomous and semi-autonomous automobiles and even aeroplanes, in the recent months. Autonomous cars rely heavily on wireless networks and satellites to perform their functions. By using unsecured or poorly secured methods of communications, manufacturers of autonomous cars could be inadvertently putting the users in danger.

The increasing interest from hackers in IoT devices suggests the recent attacks are just the beginning. A hacked IoT system can potentially be used as a gateway to any other connected devices, for example smart mobile phones, or enterprise infrastructure. Once attackers are inside an IoT system, they might have the ability to transmit malicious code through the IoT communication system to any connected devices or systems. Unless device developers and manufacturers provided this issue the attention it deserves, we anticipate that IoT hacking will become more mainstream route of attack among hackers trying to infiltrate enterprise networks.

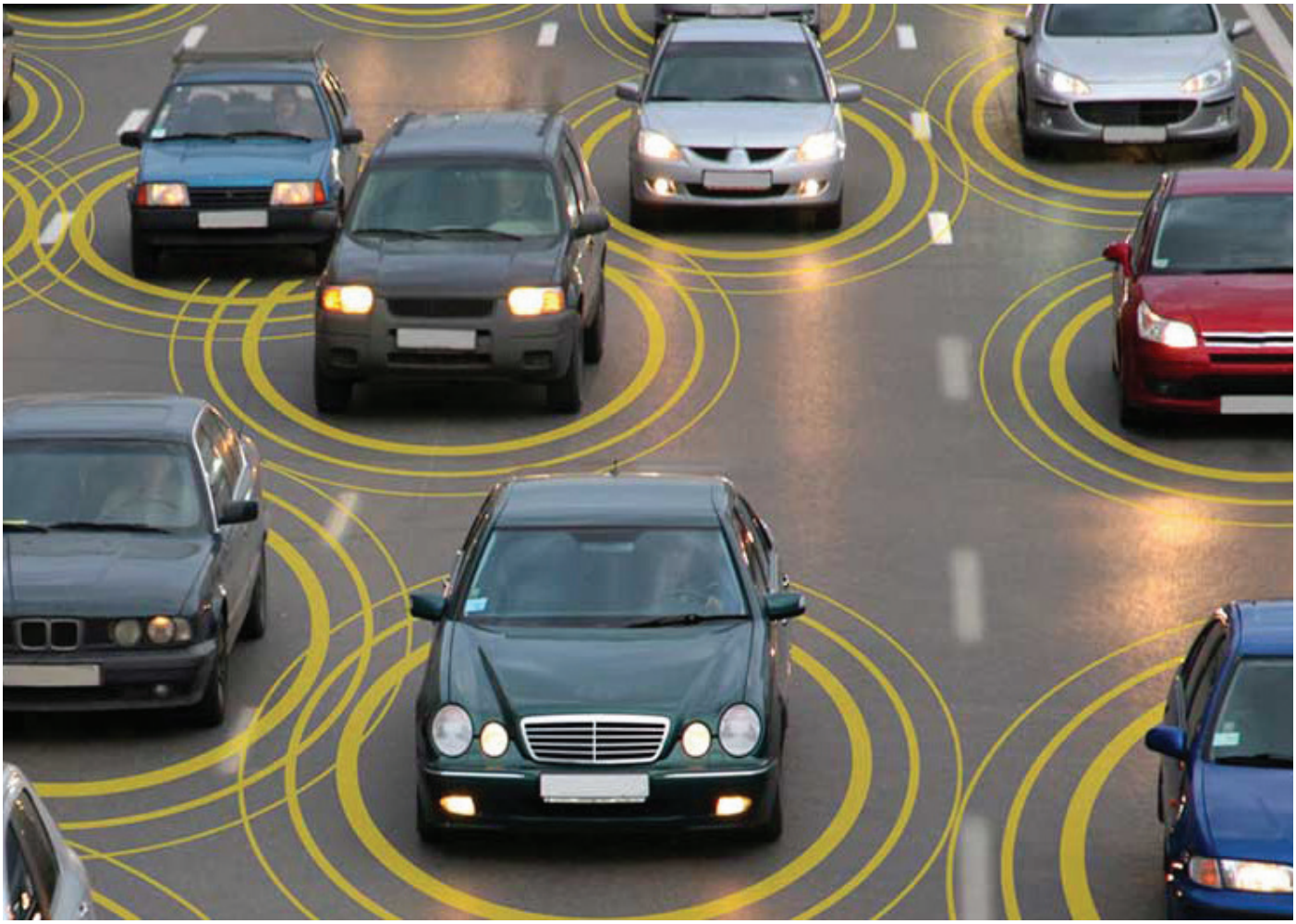
Ultimately consumers of IoT products also have a responsibility to play their part in securing their devices. When it comes to smart devices, it is clear that many manufacturers have been slow in issuing security software updates. However, if a device has already been exploited by an attacker, it is probable that the attacker will set the device to refuse any manufacturer updates, enabling the attacker to continue with maximum control over the device. In this scenario, it is the responsibility of the device's user to check that their devices are up to date with manufacturer updates and that they are not being unexplainably manipulated, for example being used as a botnet or as surveillance device. Virtual Assistants like Amazon's Echo and Google Home are increasingly becoming part of household's entertainment systems. These assistants contain an 'always-on' microphone, and they have the potential to act as an excellent spying device for an attacker. In addition, customer data and search history are stored on these devices. This data could be obtained by attackers, providing them with useful information about the habits and routines of a household.

In March 2017, Wikileaks claimed in leaked intelligence documents that the CIA is running a secret computer hacking program, providing its agents with tools to hack and listen into everyday devices such as TVs, phones and tablets. The report also suggested that the CIA has acquired the capability to target cars, which are operated by on board computers with Internet connectivity. Wikileaks further claimed that once in control of the vehicles, the CIA could stage a crash, resulting in an assassination but making the crash appear to be an accident. Similarly, Wired, a reputable technology news outlet reported about a hack conducted by two security researchers on Chrysler's Jeep Cherokee in 2016. The article stated "By sending carefully crafted messages on the vehicle's internal network know as a CAN Bus, they (the Security Researchers) are now able to pull off even more dangerous, unprecedented tricks like causing unintended acceleration and slamming on the car's brakes or turning the vehicle's steering wheel at any speed."

Zero day exploits are security flaws that were not previously known. Hackers are now successfully employing zero day exploits to attack devices and networks. We anticipate these type of attacks will become an even bigger problem for users, manufacturers, and Governments, compared to attacks on small immobile devices. In March 2016, the Federal Bureau of Investigation released a public announcement (I-031716-PSA) in which it warned that modern motor vehicles are increasingly susceptible to remote exploits and urged the consumers to be cautious and recommended measures to minimize the possibility of an attack.

"A hacked IoT system can potentially be used as a gateway to any other connected devices, for example smart mobile phones, or enterprise infrastructure."

Following these claims about the CIA, Wikileaks began dumping the CIA hacking tools on the Internet. They said they hoped manufacturers would study the exploits and take measures to ensure that the vulnerabilities were patched. However, the tools have ended up in public domain and are being accessed by malicious hackers, who have employed them to create even stronger capabilities to attack everyday smart devices.
In order to protect themselves, enterprises need as a minimum to adhere to security standards. Therefore, the most efficient way to ensure that your smart devices are safe and secure is by considering the four steps

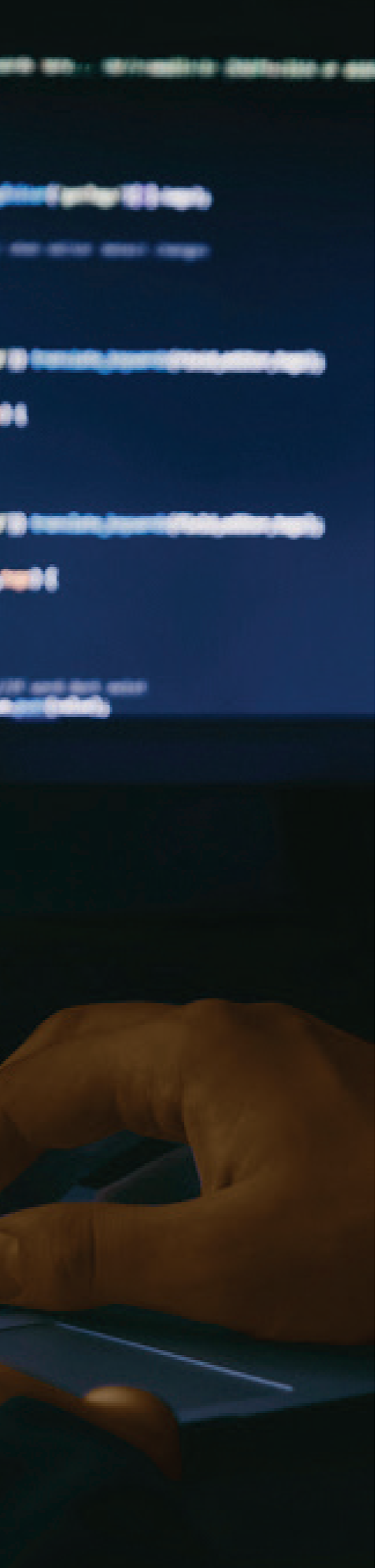


1. Making sure that Internet connected devices, connected networks and operating software are running the most up to date patch issued by the manufacturer.
2. Ensuring that all communications and data transferred over the network is encrypted. This allows the user to create a barrier between themself and an attacker.
3. It is also strongly recommended that a strong password be used wherever possible. Readily available hacking tools can easily crack weak passwords. A strong password is usually defined as having a minimum length of twelve characters, comprising of unique mixture of letters, numbers and symbols. This can reduce the possibility of your device getting hacked by an attacker.
4. Use multi-factor authentication for critical devices and infrastructure to stop unauthorized access. Dual layer authentication is also excellent mitigation mechanism to repel brute force attacks.

Periodic penetration testing exercises from an accredited security auditing company are also recommended. These tests can substantially increase the chance of discovering any potential anomalies or holes in the security of smart devices or the systems they are connected to. By simulating a real-world attack scenario, a penetration test can determine the vulnerabilities that exist in your systems, enabling you to understand and improve your ability to deal with the attack, when it occurs.

"This data can easily be obtained by attackers, providing them with useful information about the habits and routines of a household."

“8 billion currently connected IoT devices, set to rise up to 75 billion by 2025, pose a significant cyber risk to the global digital infrastructure”



Expert Analysis

The growth of IoT and mobile devices, with the capability of exchanging data over the Internet, has created the biggest digital attack vector known to the technology industry in recent history.

Through ongoing education, IoT developers will start taking security more seriously, but the evidence suggests that it has not happened yet. Which is why an estimated 8 billion currently connected IoT devices, set to rise up to 75 billion by 2025, pose a significant cyber risk to the global digital infrastructure.

Current attack trends should lead companies to rethink their defence strategies in the face of repeated cyber threats. As a minimum, SMEs should adhere to above mentioned security protocols and offer security training to its staff. In addition SMEs should consider committing to regular and ongoing training to increase staff awareness of security issues and take part in regular security auditing and penetration testing exercises, to reduce the likelihood of becoming a victim of social engineering attacks.

Dell, one of the most recognizable names in IT, serving corporations and end users of all types. Their 2016 annual cyber security threat report showed a worrying but unsurprising surge in the cyber crimes that are being committed across the globe. Their report demonstrated the severity and magnitude of the ever-increasing attacks on big names, such as Amazon, Bank of Scotland, Ashley Madison, Harvard University and many more. Overall, the report by Dell presented an alarming rate with which viruses, Trojans and increasingly sophisticated exploit kits are being used to target computing and IoT devices. However, critical servers currently remain the primary target of the attackers in the category of intrusion attacks.

Another company, FireEye who focus exclusively on the cyber security, published their report in early 2017 on the emerging trends in attack methodology employed by malicious attackers and digital defence strategies. FireEye commented on the rise of sophisticated attack methods, stating

"Financial attackers have improved their tactics, techniques and procedures (UPS) to the point where they have become difficult to detect and challenging to investigate and remediate."

The research conducted by FireEye also highlights how hackers are changing their tactics to bypass complex authentication protocols. For instance, attackers are increasingly developing malicious applications that can overcome two-factor authentication requirements by embedding malicious applications with Open Authentication (OAuth) tokens. OAuth is an open-source standard and is widely used by developers to obtain authority to share information without the need for a password. If a victim mistakenly authorizes the malicious application's request for access, the attacker acquires the ability to gain access to all data held on victim's account, for example their Google account. Additionally, the attacker can retain the permission to access the account, even if the password is updated or changed.

FireEye found that it in 2012 it took 243 to discover that a breach had occurred. More recently, this time period has reduced slightly, though by any measure, two hundred days is a considerable amount of time for anyone to monitor your IT network, potentially extracting and analysing your data.

Though we are making progress when it comes to attacks being detected and remedied, regular audits and penetration testing exercises can help to find these breaches earlier. The next section of this white paper will shed some light on the benefits of regular penetration testing.

"Infosecurity, Europe's largest Security event organizer, stated in their magazine: "Hackers spend 200+ days inside [an IT] system before discovery.""

"Rapid expansion of IoT devices coupled with inadequate security mechanisms employed by these devices..."

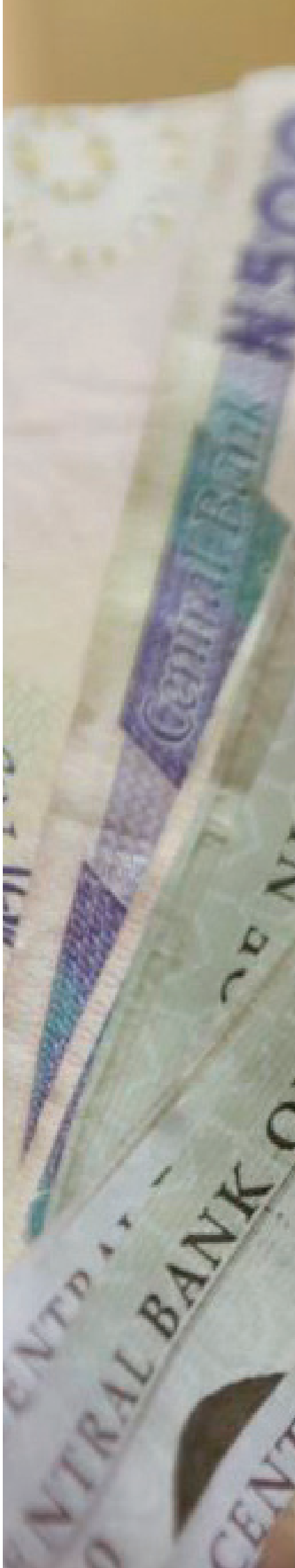
Value of Penetration Testing

In today's convoluted security landscape, it can be hard for businesses to keep track of all the emerging threats.

As more and more zero day exploits are exposed by the researchers, it is more important than ever to have an understanding of what issues a business might suffer, if they face an attack on their infrastructure.

During an attack, companies may suffer loss of their services. In the aftermath of the attack, as well as suffering loss of reputation, companies can also receive fines from regulatory authorities if they failed to to take sufficient steps to protect their systems. Additionally, further problems can also arise if customer data is lost, this can include reputation damage, as well as the threat of lawsuits from customers. So, to protect an enterprise from the possibility of an attack, penetration testing is a regular exercise which is undertaken by security professionals to find and assess vulnerabilities in an IT infrastructure or system. Penetration testing is essentially the practice of testing the system against potential known technical weaknesses, to determine the type of vulnerabilities residing in the software, hardware and web applications.

The main purpose of the exercise is to find vulnerabilities, and inform the enterprise of any actions that can be taken to remove the vulnerabilities, resulting in it being more difficult for anyone, particularly malicious attackers to gain access to your infrastructure and data. After completion of the testing, the penetration tester prepares a detailed report with a list of all vulnerabilities that were identified, followed by a set of recommendations. This report enables the enterprise to take the required steps to fix or patch any technical or procedural weakness in their infrastructure.



"A company loss of ₦1,801,637,800 is a substantial amount. In contrast, security testing would only cost a fraction of this amount."

Advantages of Periodic Penetration Testing

It is reported by Navigant, a specialized expert service firm, that the average cost to an enterprise as a result of a security breach in 2013 was £4,976,900, equivalent to ₦1,801,637,800. Navigant also reported that the security testing performed by 'Cenzic Security' in the same year, led to discovery of technical flaws in 96% of the cases. A company loss of ₦1,801,637,800 is a substantial amount, in contrast, security testing costs a fraction of this amount. These incredible figures demonstrate a strong case for why corporations must integrate regular penetration testing into their security procedures.

It is recommended that these security evaluation are repeated periodically, especially during the creation of a new infrastructure or significant alteration to an organization's IT infrastructure. If the evaluation cannot be carried out during an alteration phase, it should be carried out after shortly after its completion to highlight new vulnerabilities. A detailed penetration test provides the following benefits to the client:

1. Testing of defence capability: One of the primary reasons corporations get their infrastructure tested is to determine vulnerabilities on their systems. A penetration test not only reveals the flaws that can be exploited by attacks, but the assessment can also help the organization understand their readiness to deal with a breach if an attack occurs.
2. Compliance and Certification: Penetration testing can assist an organization to achieve certifications for example, ISO 27001 or geographical and industry compliance or regulation. These certification can a legal requirement for corporations and businesses. Security testing can include testing specific to these certifications if required.
3. Market Competition: To be competitive in the market, SMEs often have to demonstrate they have taken sufficient security precautions, for example protection of data or disaster recovery plans. A certificate demonstrating security auditing and penetration test can help assure customers the enterprise is responsible, and taking necessary security steps.
4. Risk Assessment: Another benefit of periodic penetration testing is to satisfy Risk Assessments defined within business plans or project life cycles. It is important for SMEs to have a risk-aware approach, demonstrating a good understanding of information security. Penetration testing can help an organization to understand the weaknesses in their technical infrastructure. Additionally, the penetration testing final report comprises of an extensive list of recommendations that enterprises can implement to strengthen their system. This list of recommendations will be graded to differentiate the effect that each recommendation can have on the system's security.

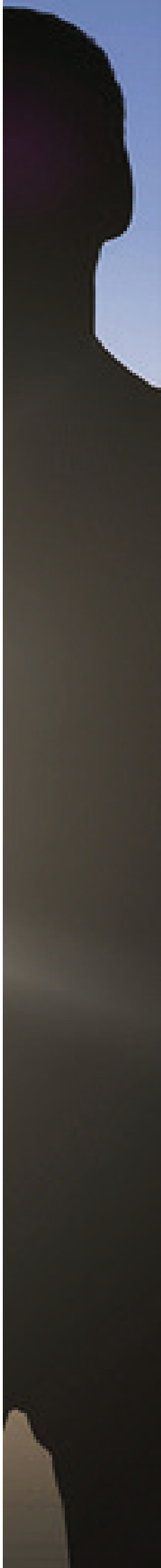
In short, not only do corporations need to take the four steps listed above to strengthen their systems, they need to go above and beyond normal business practices to stay on top of security threats which are continually evolving. The security challenges in today's digital world are dynamic, daunting and convoluted. Therefore, robust cyber security, continual testing of infrastructure and regular training regarding the security outlook of employees should be the top priority of all corporation that have an IT infrastructure, not just those who want to be security conscious. A holistic and comprehensive strategy that deals with risk management, cyber security and continuous penetrations testing, will help the businesses in protecting themselves from the dangers of cyber attacks. Chert Security is here to support you in this journey.

Cyber Threat Predictions

Short to long term insight for companies looking to stay ahead in the race against cyber attackers. The content below predicts the key development and forecast trends that are likely to occur over the next few years.

1. Ransomware: The availability of beginner-friendly ransomware deployment kits has enabled even the low-tech criminals or disgruntled employees to enter sphere of cyber crime. This is likely to increase, resulting in an increase in Ransomware attacks on technology users of all types.
2. Data Breaches: With recent attacks on LinkedIn, Target, Wonga, NSA, Cloudflare, CloudPets and many more, attackers are actively targeting institutions and corporations for user data and information. We anticipate that in the coming years, this trend is likely to continue with many more organized cyber assaults on consumer data organizations.
3. Phishing attacks: Software as a Service (SaaS) cloud model, which enables enterprises to purchase software that is accessed through a cloud portal. SaaS is particularly susceptible to phishing and server cracking attacks. Over the last few years, we have seen advances in the complexity of phishing attacks. Criminals now have the ability to forge SSL certificates, which renders built-in browser protection useless against phishing. Because of the ease with which certificates can now be forged, we predict substantially more attacks, as more businesses move their data to cloud based solutions.
4. State-sponsored attacks: In the light of recent attacks including Stuxnet, The Shadow Brokers Leaks, North Korea Hacks, we believe will continue to witness an increase in state-sponsored or state-supported attacks, particularly as Government's desire to know more about what their International friends and foes are doing.
5. Smart Grid and IoT: In the recent years, there has been a significant rise in the adoption of smart grid and IoT devices. Many cities are now competing to implement smart features in their infrastructure. However, this technology suffers from serious vulnerabilities. As the uptake of this technology increases, attackers will have increased number of vulnerable of devices and appliances, which can they could attack for malicious purposes.

To protect oneself from ever increasing threats of cyber attacks, enterprises and end users needs to be ready with effective defence strategies. By efficiently utilizing technical and human resources to protect the network and connected devices, companies will not only protect themselves from harm and potential financial loss, but also play their part in making cyberspace more secure and safe online users. In short, the more enterprises learn about threat prevention, detection and response, the more effective they will become at preventing and mitigating cyber attacks.



Chert Security - Overview of Services

In today's growing digital world, protecting your company's applications, information and infrastructure is becoming increasingly challenging. Cyber criminals are becoming more innovative with new attacks, and technologies such as IoT, Cloud, Visualization and Collaboration tools create more vulnerabilities, that can expose your business to more attacks. Chert Security has responded to these security challenges by providing affordable and dynamic services that extend beyond just technology. One arm of Chert System Solutions, Chert Security is one of the fastest growing Technology Security Solutions Providers, with clients from more 10 countries spread across Europe as well as Africa. Chert Security has gained enormous reputation in the security industry while helping its clients implement, innovate and improve business performance.

At Chert Security, we detect and protect organisations from cyber threats. We offer our clients end-to-end security solutions, from auditing to penetration testing, security software and hardware solutions to training on security essentials.

"There is an immense shortage of skilled security workers, which is preventing businesses from bolstering their network against attacks"

Infrastucture Penetration Testing

This is an assurance exercise that employs an authorized method of assessing the security of your computing networks, infrastructure and application weaknesses by replicating the steps an attacker might take to exploit these weaknesses. This processes combines both manual and automated techniques.

Endpoint Security

When it comes to the defense-in-depth approach of securing your network, the methods by which your employees interact with the network should not be neglected. At Chert Security we provide endpoint protection covering all major platforms including Windows, MacOS, iOS, Linux, and Android.

Vulnerability Assessment

We assess the security and integrity of your infrastructure to identify vulnerabilities that threaten to compromise the security of sensitive information. We also provide recommendations on how to improve your overall security posture.

IoT Infrastructure Penetration Testing

Whether you are checking IoT devices that are already connected to your networks, creating a new IoT product or deploying an IoT software solution, Chert Security provides advanced IoT penetration testing services to identify risk and vulnerabilities, and apply solutions to mitigate security issues across your IoT ecosystem, before attackers can take advantage of them.

Compliance

At Chert Security we understand the value of information, and how information management is pivotal to your business. We can help you to understand the compliance or legislation standards that are appropriate to your organisation and support you to achieve certification, allowing you operate your business with maximum confidence

Web Application Penetration Testing

The security of your web applications is of paramount importance to your business continuity and integrity. At Chert security we combine proven processes and highly skilled testers to identify vulnerabilities or loopholes that can be exploited in your web application.

Social Engineering

Reports show that malicious actors are often more successful at breaching a network infrastructure through social engineering than through traditional network and application exploitation. We can train your staff to reduce this route of attack.

Training

Your staff are the most expensive and valuable part of your company. At Chert Security we understand this, and we also understand that your cyber security is only as strong as your weakest link. We can help you and your team to understand information management, security hygiene techniques, good practices to avoid phishing and social engineering attacks and other area of security or data management, allowing you to focus on what you are good at.

We offer a bespoke cyber security security solution, we consider your people, culture, processes and the physical environment to make your business as impenetrable as possible against the threats from Cyber criminals. This is what has made Chert Security the ideal service provider for many SMEs.

Credits

Akin Ande

Chief Executive Officer

Akin is the founder and CEO of Chert Security. In the past Akin has been involved in multiple successful Tech companies. However, his attention is currently focused on growing Chert Security into a global player. With a vision to provide high quality and affordable service, Akin is on track to make Chert Security a well-known and reputable brand in the IT security industry.

Akin graduated as a Software Engineer from Manchester University in 2008, as well as being a family man and a father of two children. He has a passion for entrepreneurial projects and raising money for good causes.

Jibran Saleem

Cyber Security Developer

Jibran joined the company as a Cyber Security Security Developer after completing his MSc in Computer & Network Security from Manchester Metropolitan University.

Jibran previously held the position of System Administrator at HSBC and won numerous awards for his work. Jibran is a technology enthusiast with interest in penetration testing, IoT and network defenses.

Daniel Adebayo

Senior Security Consultant

Daniel is a Senior Security Consultant at Chert Security with a passion for information security. Previously a Network Engineer, Daniel has dedicated his career to designing and securing information systems

Daniel earned his B.Sc at Covenant University, amongst other certifications he holds a CCIE, CEH, PCNSE, CCSA and OSCP.

Special Thanks

Ruth Irwin

Dr. Mohammed Hammoudeh

Feyi Ogunkunle

Toyinsola Oduyale

2018

CHERT SECURITY

www.chertsecurity.com