THE ULTIMATE GUIDE TO SECURITY AWARENESS TRAINING

Cyber Risk Aware

Creating your human firewall!

Cyber Risk Aware

Creating your human firewall!

Cyber Risk Aware
Creating your human firewall!

THE ULTIMATE GUIDE TO SECURITY AWARENESS TRAINING

Index

INTRODUCTION TO INFORMATION SECURITY

Introduction to Information Security

The use of technology is an inescapable component of modern business operations. From manufacturing to marketing, sales to finance, and every aspect of communications therein, technology plays an ever-increasing role.

Yet the risks associated with technology are well known. A recent report in the Atlantic found that 92% of IT firms have reported attacks on their clients' systems[1]. The dangers of leaving computers unprotected and their respective systems and data vulnerable, have cost companies millions of pounds per year. Therefore the impetus is on proactive management teams to guide their staff, through policies and training, on the critical importance of cyber security.

Consider the 2017 Equifax breach, in which, over a period of several months, millions of consumers were impacted. The company was initially warned that they needed to patch a software vulnerability, but their IT team did not follow the required protocol. They ran scans that should have detected the vulnerability but didn't. Believing they were safe, business went on as usual.

Then on May 13, hackers gained access to the Equifax servers, reportedly via one member of staff. The hackers then instantly had information, including: social security numbers, private financial data, and addresses for over 143 million people. The attack would only grow from that point on, demonstrating how a seemingly small security flaw can become one of the largest and perhaps costliest attacks in history.

There are thousands of stories of various scale, from businesses across the globe. Far and wide, cyber attacks and data breaches have increased in frequency and extent, and one has only to look at the aftermath of many of these disasters, to be prompted into action.

For example, here is 2018, 5 years after the Target super-store data breach; the company is still dealing with the ramifications of their security incident. Not only has Target spent upwards of 140 million pounds[1] on their cleanup efforts and legal fines, but their settlement includes a requirement to strengthen their security program: including hiring a Chief Information Security Officer, improving security processes, and establishing a security training program for their staff.

[1] https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

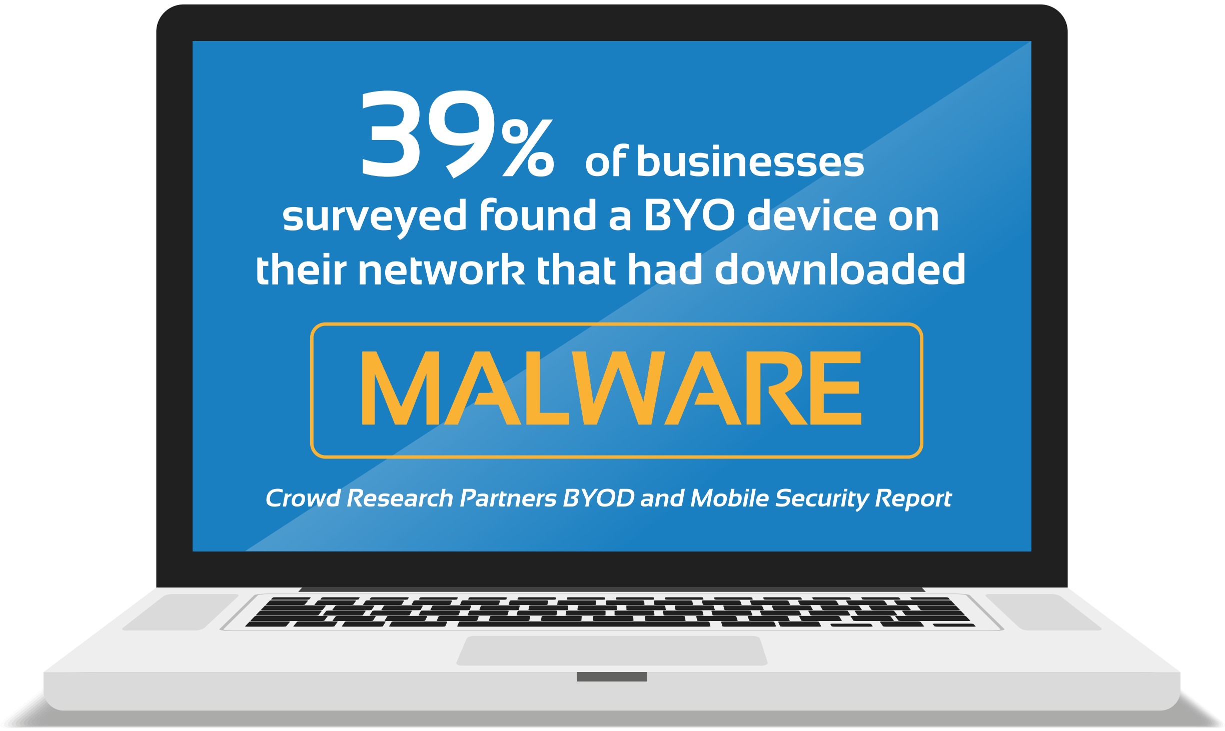
Research released by the Global Cyber Security Capacity Centre affirms the indisputable importance of training in mitigating security risk. [2] It is only through committing to a comprehensive training program, one that will guide individuals on the elements of data safety, that organisational protection is possible.

Our team at Cyber Risk Aware has decades of experience in the IT security industry. We've worked with clients across the globe in building security-training programs that safeguard their systems and support their teams. We're now providing you with the tools to help your team meet its security objectives in the coming years. This guide will help provide a clear answer to this question and introduce you to the most strategies for mitigating threats to your company's security. In the following pages you'll learn more on:

- **Understanding the modern cyber security landscape**
- **The techniques hackers use to gain entry to your systems**
- **The threats facing your company and its customers**
- **The value of a security awareness training program**
- **The key elements of a robust security awareness training program**
- **The best practices for commencing and sustaining security training**[2]

[2] https://www.csoonline.com/article/3229969/data-breach/awareness-training-is-key-to-reducing-securityrisk.html
https://www.theatlantic.com/business/archive/2016/09/ransomware-us/498602/

UNDERSTANDING THE CYBER SECURITY LANDSCAPE



39% of businesses surveyed found a BYO device on their network that had downloaded MALWARE

Crowd Research Partners BYOD and Mobile Security Report

As we come to depend more on technology in business as within our day-to-day lives, the threat to our systems is evolving. We've moved on from simple viruses that attack a vulnerable PC leading to hours of removal and repair work. We're now in an era where the wireless technology is being used to control devices across the organisation; where each individual has their own smart phone. Now, each team member has their own role to play in protecting their organisation and its customers from outside threats. And so, the question becomes: What can organisations do to empower and guide individuals in supporting organisational security in this era of increased digital dependency?

AN EVOLVING THREAT

With an increasing consumer awareness on security breaches and data risks, companies must now be more proactive in how they manage their systems. The studies show that cyber-attacks are increasing in both frequency and scale. Research by digital services company Gemalto found the number of data breaches worldwide increased by 164% between 2016 and 2017[3]. And many growing companies across the country are still not prepared to face the new and emerging threats.

Let's look at the factors that are influencing the current cyber security landscape and shaping the marketplace.

[3] https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html

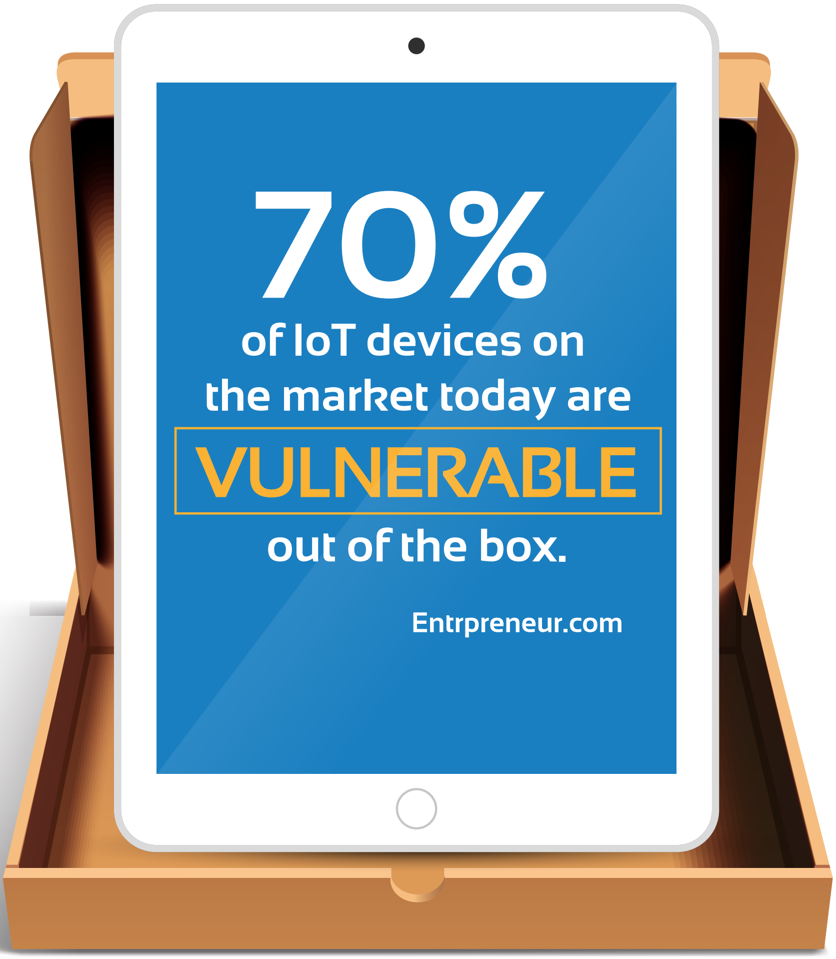
DEVICE CHANGES

The diversity and number of devices that both employees and customers of the modernorganisation use is increasing. Whether it's the latest iOS system or the newest Android release, mobile devices are now increasingly being targeted by hackers directly as a way to access business information and extract valuable data.

The newest devices might feature the latest security protocols, but companies must still put safeguards in place, and educate employees on the benefits of their use. This is particularly true within an organisation with a BYOD policy, where outside devices are being brought into the office. Policies of this nature might give employees more flexibility and autonomy within their positions, but they also present a threat to companies in which data control and access limitations are critical security considerations.

THE IoT

The Internet of Things is a developing marketplace in which every item within the office, from the thermostat to the refrigerator, is connected to the Internet to provide a constant data link that helps automate various elements of office life. While this increasing automation is making the life of the modern employee easier, and helping companies reduce costs, it also presents a very real security risk.



In an environment where many systems are connected to the same server, it only takes a small flaw in a rarely used product to allow access to the entire data infrastructure. And, all too often, connected devices are left vulnerable through the use of default passwords, and standard security protocols that have long since been infiltrated by hackers.

The IoT trend has given rise to the looming threat of botnets, which are automated systems that scan large swaths of information in seconds for potential weaknesses. Botnets use default passwords and other standard security processes to log-in to unprotected devices, allowing them to control the device after entry and then use the data they find to impact the company, its staff and employees.

In capitalising on the IoT trends within their companies, teams must maintain clear sight on their security goals and mitigate the impact of automation on their security structure.

LACK OF ONSITE SKILLS

With the increasing need for IT security guidance and the rising challenges emanating from across the globe, there's a dearth of onsite skills for the modern business to utilise. Specialists in IT security, particularly in modern IT security threats are few and far between.

Recent data shows that 75% of organisations worldwide lack a cybersecurity expert on their staff[4]. And this is leading companies to turn to outside sources for a response to the challenge. It's the reason many are outsourcing their security education and working with trusted companies in ensuring their IT teams and other office staff have the information they need to make more effective security choices.

NEW FORMS OF ATTACK

In recent years, attackers have also devised novel ways in which to attack organisations and access data. One of the more common methods in large-scale attacks in recent years has been the use of ransomware. Ransomware attacks involve infecting an organisation's systems and then asking for a form of "ransom" in order to stop the attack and remove the infection.

The success of these types of attacks was highlighted by the WannaCry event, in which 250,000 computers in over 150 countries, including systems in 16 NHS medical centers, were infected within less than a day.[5] As with the Equifax breach, a patch would have resolved the issue but, without a proactive focus on IT security, organisations incurred a significant cost.

Business email compromise is another form of attack that is on the rise in recent years. The data shows that between October 2013 and December 2016, hackers stole over $5.3billion in the U.S. alone through BEC attacks. [6] This style of threat is becoming more popular along with BYOD policies. Companies allowing their employees to bring their own devices must be acutely aware of the importance of email security and threat analysis.

Many experienced professionals have fallen victim to sophisticated email attacks in recent years, simply due to a lack of education within organisations and a lack of attention to detail. The goal for the modern company is to train employees to identify out of the ordinary requests and common strategies used by attackers to gain data access.

Prediction Models an Important Security Element within the current security field, AI-based prediction modeling has become another important element in safeguarding companies against potential threats. Studies involving the use of AI-based machine learning programs are helping to determine when an organisation is most vulnerable to attacks and through which channel a threat might be arise. This can give companies the upper hand in terms of defending their data and in threatmitigation over the coming years. The focus is now on helping staff work with these machine learning systems and on learning the measures to take when a threat is highlighted.

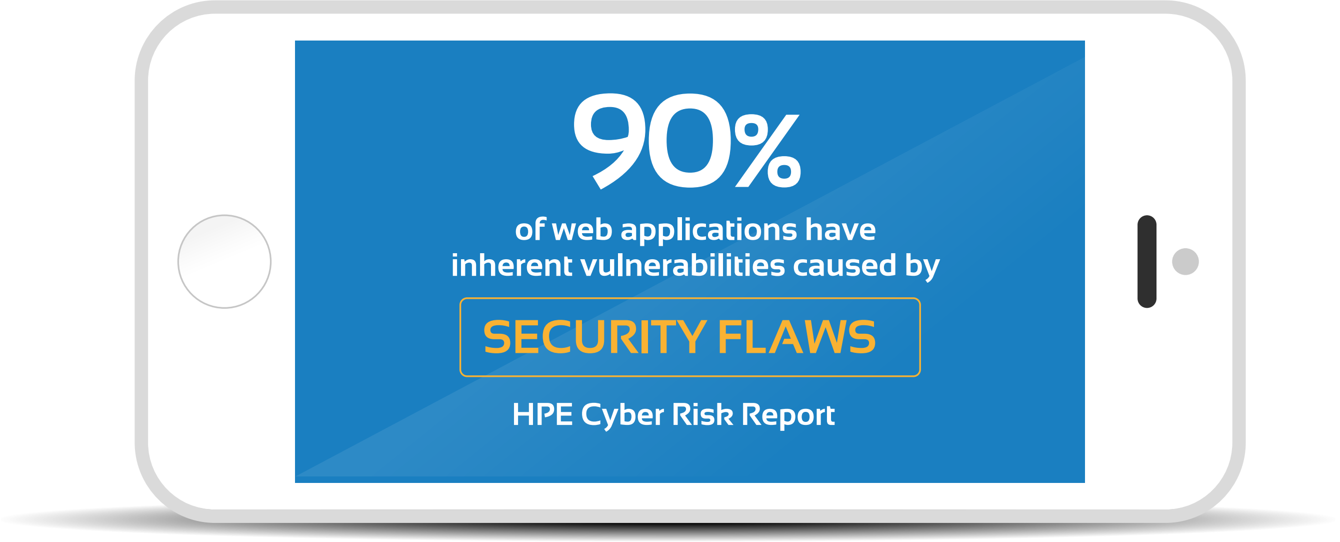
[4] https://www.securitymagazine.com/articles/87527-percent-of-organizations-lack-skilled-cybersecurity-experts

[5] https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/wannacry-ransomware-attacks/

[6] http://www.eweek.com/security/business-email-compromise-scams-continue-to-grow-with-5.3b-in-losses

USE OF APPLICATIONS AS A THREAT

While mobile applications are now helping improve the performance of smartphone and increasing the capabilities at the hands of the mobile workforce, the data on mobile applications is at significant risk of attack in the modern area. Many organisations are now harnessing sever-less apps, which support greater scalability. These applications also capitalise on the use of data in transit. Data being sent between networks is at its most vulnerable state and can be captured by coordinated attacks seeking out specification information on a company, its employees and customers. The use of applications within their workforce can make companies more vulnerable to DDOS attacks, in which a server-less architecture might fail to scale with the demand for service, leading to expensive disruptions for the company.



90%

of web applications have
inherent vulnerabilities caused by

SECURITY FLAWS

HPE Cyber Risk Report

HOW SECURITY BREACHES OCCUR

PERSONAL DATA
58%
of UK companies
have reported
DATA
BREACHES
in the last two years
GFI Software and Infinigate UK

How Security Breaches Occur

In learning more on information security, business leaders must first study the most common types of security breaches and how orgnisations have been impacted by these events. The following are common techniques that attackers use to breach the security of the modern company.

SQL ATTACKS

SQL attacks are considered the low-hanging fruit of the security field, as they are one of the easiest to prevent and yet remain among the most common techniques deployed by attackers. The SQL attack allows a hacker to enter malicious code in a piece of text, perhaps in an email or a Word document. The malicious code then allows the attacker to take over the device and extract specific data. Using this technique, cyber criminals have been able to gain access to company financial information, customer data, and other high-value items that might be stored on a server.

STOLEN PASSWORDS

Another common way in which attackers gain access to information is by stealing passwords from a company directory. They might gain access via a traditional SQL attack or by simply by using social engineering to acquire information over the phone. Teams must learn more on how social engineering is being used to gain access to information. In this scenario, a person may call and say they are from the firm's IT security department and require access to login credentials to update their computer. In many cases, employees simply trust the person on the phone and provide their details of their own free will.

A password can also be stolen easily if the user has kept their default password or if the password hasn't been updated regularly. Hackers are now using botnets to brute force attacks using default passwords on millions of computers over a short space of time. Keeping the default username and password on the device leaves the user vulnerable to password theft and data loss.

MALWARE INSTALLATION

Another common form of attack in recent years is through the use of malware. Malware is a form of malicious software that, when installed on the target system, can be used to control system data and allow the attacker to steal all available information. The malware is often installed after an email is sent to the target. The email is usually designed to look as if it came from an authority within the company or a software manufacturer offering an update. By accidentally installing malware on their computer systems, users can then allow the malware to spread throughout the company's network, infiltrating all data areas and causing significant issues. It's part of the reason that companies are now educating their employees on how to spot the signs of a malware infestation and guiding them on mitigating the issue before it begins to cost the company and its customers.

DEVICE THEFT

In the BYOD era, companies are now giving mobile staff members the option of bringing their device with them and then using their personal device to communicate with customers and other employees. Data retained on these devices has become highly valuable to attackers as it often contains the credentials for logging into secure areas of the company network. And so, when a device is lost or stolen, it can put the company at risk of a significant financial loss. Proactive companies are now building policies that help to safeguard data in the event of theft or loss.

They are also encouraging employees to back-up their device data on cloud-based system to mitigate the threat and implementing BYOD policies such as document protection to ensure lost devices don't lead to further financial loss for the company.

65%

of companies don't enforce their password policy

Ponemon Institute

DOCUMENTATION ERRORS

Human error is another of the leading causes of security issues within the modern organisation. With the vast amount of documentation being disseminated throughout the globe, companies are now focused on using these documents effectively and preventing private document data from getting into the hands of cyber criminals. Oftentimes, a security breach within a large company is the result of a simple documentation error by an employee.

The employee might simply make the mistake of publishing private data on a public resource,giving access to a website or the email address of a company employee which then leaves their data vulnerable. The forwarding of sensitive information is another common mistake. Choosing the wrong email address or adding information that should have remained on a private server to the email chain can have a significant impact on the company. It's why so many are now taking the time to teach their employees about how to work with documents and how to control the flow of information from their computer.

FAILURE TO BACK UP DATA

The failure to back up the data on the server could make a security breach costlier when teams have to add the data back into the system. Many security breaches not only result in the theft of data but also the loss of data for the company. In the case of a stolen device for example, this could leave the team with no understanding on which data was lost and who has been impacted. Take the time to back up data regularly and find out who is using which data on the system. This data retention process can help create a chain of custody for the data and prevent significant costs being incurred in the future. In view of these threats, what can companies do to safeguard their data? There are multiple steps that should be followed in ensuring that data is safe and security breaches are eliminated. Our team at Cyber Risk Aware specialises in advising companies on IT security and we recommend the following steps be taken to prevent data breaches:

- **Institute end user awareness training through a qualified company**
- **Craft a comprehensive encryption policy**
- **Perform regular vulnerability reviews with the team**
- **Apply patches regularly and review new patch options**
- **Back up all data regularly**

THE THREATS FACING YOUR ORGANISATION

In safeguarding their company in the current landscape, business leaders must learn more on the common threats to their organisation and its data. Each industry faces varied risks from threat actors, each with their own motivation and intent. As leaders in the cyber security marketplace, Cyber Risk Aware staff regularly work with our clients in mitigating threats to their business and we have found the following threats to become a growing issue within today's organisations:

MAN IN THE MIDDLE ATTACKS

One of the more common modern techniques hackers use is a sophisticated version of the traditional man in the middle attack. The attacker finds their way into the organisation and then places a keylogger or another tracking system on a computer. New attacks use IOT devices to listen in on all wireless communications across the network. They then gain access to a company email address and watch the communications that take place between the user and others in the company. Because they have access to the user's credentials and their passwords, they can then act as the person in emailing others for financial information and private data.

PHISHING SCAMS

A recent phishing scam conducted by a Lithuanian cyber-criminal cost Facebook and Google more than $100 milliion combined[7]. There are still rich rewards for phishing attacks and firms must be prepared to mitigate the issue. Companies continually fall victim to phishing scams, despite this technique being one of the more common and widely understood issue within the security marketplace. The typical phishing attempt involves a simple email which is designed to look like it came from an authority within the company. The email might ask the person to download a document or click a link within the content. Once the desired action has been completed, the attacker is given control of the device and can then access device data and act as the user of the system.

BOTNETS

A botnet attack begins with a single computer virus. The virus then spreads to connected computers on the network, and then sends a signal back to its command center, which is operated by the cyber-criminal. From their command center, the criminal can then control all the computers within the botnet, and use any data they discover as the review the network. Botnet attacks are on the rise across the globe and many skilled hackers are even now offer botnets for hire for others to use. It's a billion-pound industry that is only set to grow with the increasing success of botnet events.

MALICIOUS JAVASCRIPT

The websites that we click on every day during work hours can detail specific information about our location and our computer. Those with criminal intent can create sites that have a malicious JavaScript written into the programming to allow the instant download of a virus once the user opens the site. One click from a user within a company network can cause the download of a virus that shuts down the entire network, and potentially costs the company thousands of pounds in lost revenue. This is yet another reason behind the importance of secure web use and for installing the latest virus scanning and removal products.

[7] http://mashable.com/2017/04/28/google-facebook-email-fraud/#2xmPdw5nLqqM

HARNESSING THE VALUE OF SECURITY AWARENESS TRAINING

> Training employees how to recognize and defend against cyber-attacks is the most under spent sector of the cybersecurity industry."
>
> *John P. Mello Jr. – Tech Beacon*

With the wide-ranging threats facing organisations in the modern business climate, the need to educate employees is clear. But most companies still have little understanding on the importance that a comprehensive employee-training program can bring to their business and so here our experts will lay out the value provided through security training

PROTECTING THE BUSINESS

The latest threats from computer hackers are designed to impact your business and steal money and data. Only through a proactive approach to security awareness training can companies ensure that each team member is security savvy. Security awareness training can help keep businesses running effectively when a security incident arises. Training can also help to minimise business downtime and showcase the firm's understanding of the current climate and its commitment to protecting customers and employees.

REMOVE THE WEAKEST LINK

While the technology teams use is often designed with the goal of mitigating threats and ensuring business safety, those using the technology aren't always adept in effective security practices. One of the key benefits of working with a training specialist on a security awareness program is that it removes the weakest link within your security infrastructure – the employee.

It provides the individual with the knowledge they need to detect and stop threats before they impact the business. By empowering the employee to take the measures required to protect the company, firms are now minimising the potential for attackers to target individuals. After training is completed, problems related to social engineering and other individually-focused attacks can be reduced.

CONSISTENT APPROACH

A lead benefit of security training is that it keeps every team member is on the same page when it comes to security. When a threat arises, each team member will know exactly what the process is for dealing with the problem effectively. While the burden of responsibility is still on the individual employee, they are given the tools and resources required to act on potential threats. Team members can work together in resolving security issues, building an environment of trust and confidence among coworkers.

A FOCUS ON PREVENTION

Prevention is far more affordable than responding to a security issue. Companies can save millions of pounds by using security awareness training to prevent potential attacks on their systems. Security awareness training is the ideal investment for the growing business intent on harnessing the newest technology.

SPEEDIER DETECTION

In the event that hackers try to access company data or use any of the more common techniques such as phishing, man in the middle attacks, and social engineering, trained employees will be able to detect and report a security incident in a much more efficient manner. Their security training, awareness, and vigilance will allow them to notice the changes that have taken place on their system as a result of their training, and they can then alert their managers who will initiate the appropriate response process.

> The average 10,000-employee company spends $3.7 million a year on dealing with phishing attacks
>
> ***Ponemon***

Outlining Key Features in Your Security Awareness Training Program

In considering security-training companies, business leaders must take into consideration the style ofprogram offered by the firm. Only quality programs can ensure the best return on investment in security training. Let's look at the key features of a comprehensive security awareness-training program:

INCORPORATE A VARIETY OF TOOLS

The leading security awareness training programs incorporate a range of tools and content to get the message across. From quizzes to hand-on training services, programs should be diverse to incorporate all the methods employees require for education on security.

INTEGRATED TESTING

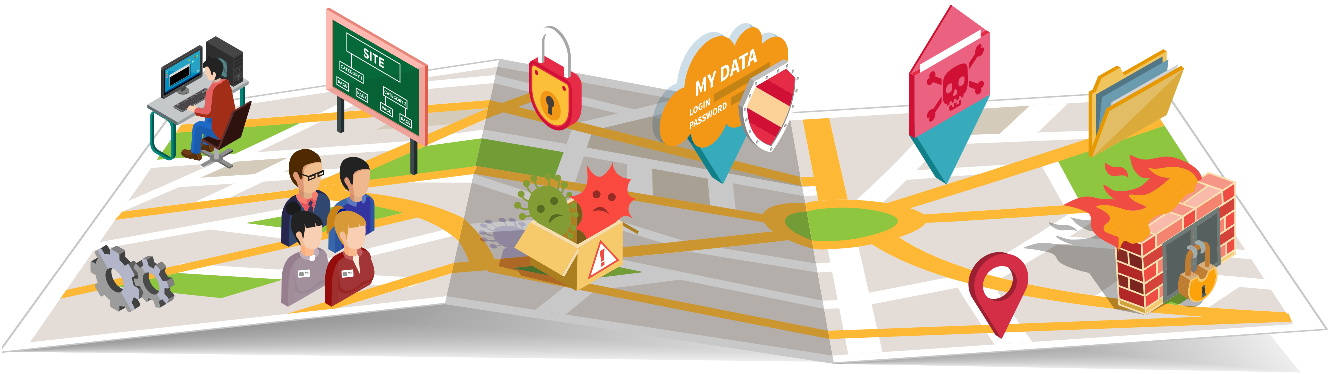
The top companies completing awareness training offer integrated testing measures that simulate a security event and test the teams based on their response to the simulated threat. Such testing has proven critical in improving team knowledge and giving management staff a clear understanding on the points-of-weakness within the organisation.

REGULAR TRAINING

The training program should include regular education classes to give employees the opportunity to build their understanding on a week-by-week basis. Conducting short, regular training over the long-term has been shown to increase user understanding and help teams remember key training elements during their everyday activities.

SECURITY ROLES ASSIGNMENT

Additional training should be provided for those in management positions in order to oversee employee actions and deliver maximum return on investment. Management teams should be trained on the steps required to help team members move forward within simulations and testing. They should also undergo training on the actions required when real-time security issues are reported by team members.



COMPREHENSIVE REPORTING FEATURES

The training programs featuring built-in reporting tools help provide actionable data on the strength of the company's security, and ensure the information is available to decision-makers. This helps to significantly enhance the value of the program and support team members in meeting their security goals. Reporting tools allow teams to see in clear detail where room for improvement exists and then to target these areas in upcoming training.

GUIDANCE ON REAL-TIME ACTIONS

The training should prepare all individuals on how to respond to real-time security issues and help them take active steps in managing the issue the moment it occurs. One of the key benefits of security awareness training is in reducing the time it takes to respond to a security threat. The best programs guide team members on immediate responses to real-time events and help teams build a comprehensive policy for protecting data and hardware in real-time when a security issue arises.

UPDATES ON THE SECURITY ENVIRONMENT

Through their regular training, employees will also be able to learn more on the security environment as it evolves. In a fast-paced marketplace such as this, it can be difficult to track and respond to the latest threats with a one-off course. A regular training course allows the specialist to help guide employees on new issues facing companies in their sector. Whether it's a new botnet or a new piece of malware, knowing what to look for can help mitigate potential damage within the business.

TRAIN OUTSIDE THE BOX

Implement gamification techniques into your training plans. Challenge your training participants to take on the mission of security; use real world scenarios for them to encounter obstacles and then have to role play the decision of what to do next. By inserting themselves into these scenarios, they will be actively engaging in security practice and learning through hands on experience how they themselves would or should act. Also, take the opportunity to offer recognition of participant accomplishments, whether it be through email communication, by awarding a certificate, or by whatever is feasible at your organization.

REFINED SECURITY AWARENESS TRAINING

BEST PRACTICES CHECKLIST

REFINED SECURITY AWARENESS TRAINING - BEST PRACTICES CHECKLIST

Armed with the knowledge on the content of a quality security awareness-training program,companies can now better select the ideal program for their teams. But success within the training program can only be achieved by building the ideal team environment within the individual business. Let's review a checklist to the best practices for creating and supporting a security-training program.

PARTNER ACROSS DEPARTMENTS

A critical element of security awareness training is partnering between and across departments so that performance goals can be shared and agreed upon. For example, make sure that HR teams are involved within the security training procedures so they can then integrate those training elements within the new employee onboarding process. Beyond this however, it is also important to combine shared needs and interests across departments. Security is everyone's responsibility, but the facets of that responsibility are shared across departments. HR departments may be tasked with safeguarding employee data, Legal departments with third party assessments and contracts, IT with system upkeep, other departments with proprietary, sales, or consumer data, and so on.

A comprehensive solution can only be built when a full assessment of the current risks and vulnerabilities are carried out. Those at the executive levels should also be kept aware of the training and have the opportunity for input to keep the program moving in the most effective direction for the organisation. Getting each member of the team on the same page regarding security will minimise confusion and create an environment of streamlined communication and cross-department cooperation.

LISTEN TO YOUR STAFF

It is worthwhile to survey staff periodically, not only to get an understanding of their vantage point on existing security risks at the employee level, but to hear about specific vulnerabilities or incidents that they may have experienced. Additionally, it is important to gauge whether every corner of an organization is receiving the appropriate security message. Is security a priority to them, to their managers and team, etc.

INCENTIVISE AWARENESS

One of the goals of a robust security-training program is to raise awareness and understanding of cyber threats with staff. However, in order to motivate change it is often necessary to not just punish negative behaviour, but to reward positive behaviour.

A reward system in place for employees that follow procedures and complete testing according to the training roadmap will engage staff in the success of security. Rewards should also be provided for reporting security issues and concerns in order to keep lines of communication open.

COMMIT TO MEASUREMENT

The single most important outcome of a training and awareness program is for measurable change in behaviour. It is not enough for employees to know a security guideline or process by memory, but to follow it as well. The only way to determine this is by maintaining metrics. Additionally, actionable data on the value of a company's training program can help to show board members and c-level executives the return on investment. This involves committing to the measurement of program success. For example, a company might implement a phishing simulation at the beginning of the program and then another simulation halfway through to show the progress being made. This can help solidify the program's value and increase the potential for investment in security moving forward.

USE RELEVANT DATA

Relevant data on real-time security threats is essential in implementing the training program. Teams must use the information from recent trends to showcase the importance of training and ensure appropriative security counter-measures are taken. By demonstrating the relevance of the training being provided and showing the true cost of modern threats, companies can motivate their teams and guide them towards taking the most effective approach for optimal security.

CONDUCT RANDOM SIMULATIONS

A common mistake made in security awareness training is simply using the same simulation techniques at the same time in the week. Soon, teams catch on to the simulation schedule and will be betterprepared to respond. To get a real understanding on security preparedness, conduct simulations at random times. Try not to give any advanced warning of the simulation.

Companies can gain actionable data on the success of their training through careful scheduling and comprehensive analysis.

COMMUNICATE

Communication is vital to security. Not only should clear communications be made as to expectations of security, including relevant policies and guidelines, but maintaining communication with leadership and staff will also keep those individuals engaged, informed, and vigilant.

Cyber Risk Aware
Creating your human firewall!

The Advantage of the Cyber Risk Aware Security Awareness Program

By working with our experts at Cyber Risk Aware, companies can build their ideal security awareness training program. We specialise in building programs that tackle the root cause in 90% of security incidents: human error.

Our fully integrated training platform includes the following features:

Intuitive set-up and performance

Our program is easy to set up on any computer network; training campaigns, quizzes and simulated attacks can be formed and utilised within minutes of the initial startup process being completed.

Customisation options

The customisation aspect of the Cyber Risk Aware program means that all elements can be designed based on the company and their unique program requirements. Phishing templates an be crafted according to unique branding and in-house campaign communications, simulation attachments can be formed based on company documents and emails can be spoofed for sophisticated response analysis.

Managed services

For company leaders with little time or resources to roll out security awareness directly on their systems, Cyber Risk Aware offers managed services. Our managed services are designed so that we take full control of the threat analysis and can provide clients with actionable reports on their teams and the performance of their security awareness processes around the clock.

Comprehensive customer support

Few companies can match our customer support services. We're a proudly Irish firm and can provide short response times for questions and enquiries from clients across the time zones. We recognise the value of speedy services in the security marketplace, and we're now offering the ideal service through our trusted support staff.

Quality Content

Cyber Risk Aware is dedicated to providing comprehensive training content that is at the forefront of industry needs. Our training videos are developed to be short and concise, keeping staff productive and informed in a matter of minutes.Our training content is innovative and engaging; and furthermore, is constantly refreshed to be in line with the demands of the evolving cyber threat landscape.

Tailored Content

Security concerns are global, but some topics require additional regional knowledge. Cyber Risk Aware is prepared to meet these customer needs, and offers honed trainings in topics like PCI, Data Protection (for GDPR, HIPPA, or South Africa), etc. Additionally all of our trainings are available in distinct US and UK versions, complete with correct spelling and terminology, to meet your organization's needs.

FORTIFY YOUR COMPANY & SECURE YOUR PLACE IN THE DIGITAL MARKET

Recent reports show the digital economy is growing at twice the rate of the wider economy, and contributes £97bn a year [8]. With most new businesses now dependent on their connections to the digital marketplace, there's never been a better time to initiate security awareness training.

While the headlines might show that UK businesses are set to lose billions in 2018 due to hacking, phishing and other forms of cyber-crime, the problems go beyond the headlines. Even the smallest attack can stall a business and prevent growing companies reaching their objectives for the year ahead. Data breaches are causing customer churn, loss of brand value and significant legal issues across the marketplace. No company is immune. Our team at Cyber Risk Aware offers a human-centric approach to security awareness training.

We work with individuals across the organisation to support all members of the group in protecting the business against the newest evolving threats. Take the time now to review your options alongside our trusted experts. Your proactive commitment to educating your employees and testing their security awareness can safeguard your business, support your team, and give your customers peace of mind in using your services for the coming years.

[8] http://www.telegraph.co.uk/technology/2017/03/22/tech-sector-growing-faster-uk-economy-72pc-investmentoutside/

Cyber Risk Aware

Creating your human firewall!

cyberriskaware.com