A Guide to Cyber-risk Management

By Jennifer Tonner - (Jennifer.Tonner@BGi.uk.com)

Cyber-risk - what is it?

'**Cyber risk**' **means** any **risk** of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

43% of organisations have already experienced an attack. Are you among them? Would you know? The truth is when it comes to a cyber attack it is not a matter of if but when.

We are bombarded with so much different information and advice it is easier to tune it out than actually engage with the subject. Let's start by dispelling some myths:

- ***I'm a small company*** – *I would never be targeted*.
  In fact you are much more likely to be targeted. Criminals are rational and will pick the low hanging fruit. 52% of small firms and 66% of medium firms are targeted.
- ***If I had been hacked I would know*.**
  68% of breaches can take months to discover. Websites such as weleakinfo.com are easily searchable for a small fee. Are you brave enough to risk it?
- ***I use a third party provider for these services so I do not have to do anything*.**
  Whether you outsource your data processing or not YOU are the data controller and the buck stops with you.
- ***I just can't afford a cyber-risk management strategy*.**
  With data showing
  - an average cost per compromised record is £120
  - 47% of consumers consider 'data breach' unacceptable
  - Your inellectual property is vulnerable to on-line theft

you cannot afford NOT to have a cyber-risk management strategy in place.

Every organisation connected to the internet is vulnerable to Cyber mischief. The areas targeted can include every aspect of your business including finance, personnel, suppliers and customers, intellectual property and operations; all potentially causing financial, reputational and regulatory

damage. Cyber-risk is rated the number 1 threat to UK businesses by leading risk management experts.

How BGi.uk can help you combat this?

BGi.uk - Cyber has been created to assist the clients of BGi.uk to develop a Cyber strategy that will help reduce the likelihood of a Cyber incident occurring - and then reduce the effect of that incident.

Reports

The first step in the process is to understand where and how you might be vulnerable and the potential costs of any data or information loss. When it comes to cyber-risks it is tricky to envisage the effect of any loss. It's easy to imagine the fire engulfing your premises but not so easy to see the stealthy hacker syphoning your data to sell on the dark web - or simply to your competition.
Individual Cyber and Comparative Cyber Risk Reports – Individual cyber-risk reports can identify areas that require your immediate attention and may require action in future. Clear guidance on how you can fix (or at least minimise the effects of) weaknesses and vulnerabilities can be provided.

You do not have to be the most secure company on the planet – but you need to make sure that you are not amongst the least secure. BGi.uk can provide reports to provide a comparative analysis of your organisation with your peers/competitors that will give you an insight as to where your business stands.

Reports simulating cyber attacks on your system are also available; enabling you to see how your systems' interface will react to real life situations.

These reports can provide a score that you might consider a 'cyber credit' check which is given context by the peer to peer comparisons.

Ongoing support by re-scanning and alerting you to new threats is also available.

How do reports perform this analysis?
The reports use the registration details of a seed domain and connect this to other domains that have been registered using similar details.
All of the external Internet facing services that are being run by your organisation are then identified. This would include database and server providers, the email policy, security and configuration information that is available. This is collated and used to determine the cyber vulnerabilities of your organisation and those other organisations within your peer group.

Different Types of Risk & Vulnerability

Email Security
If you do not put easily available, inexpensive and standard email protections in place you are at much more risk of having your addresses spoofed or impersonated leaving your employees, customers, partners and suppliers open to all sorts of fraudulent activity.

Domain Registration
If you use an individual email address to register domain it is more vulnerable to social engineering attacks which might give a hacker total control of your domain. In the worst case scenario traffic to your websites could be redirected to pages designed to defraud your customers.
Example - In 2016 hackers used social engineering to hijack the domain registration details of a major Brazilian bank. The attackers created fake versions of the bank's websites and were able to harvest customer bank details and infect their machines with malware.

Known Vulnerabilities and Out of Date Services
When a vulnerability is discovered the details are made known to the public by the developers as part of their resolution process. Unfortunately attackers also share information on how to exploit these vulnerabilities.
This also relates to services which are out of date and no longer supported or maintained by its developer. This means that bugs won't be fixed and vulnerabilities will not be patched and may not even be publicly disclosed until they have been exploited by attackers.

Misconfigured Services
Misconfigured services can also be exploited. Some services should never be directly accessible from the Internet such as databases which may contain personal or sensitive commercial data or routers or network equipment
Running services which are known to be vulnerable carries a real risk of theft of data, loss of control of website, ransomware and malware: and you are responsible for any data loss.

Example – In 2018 the Marriot Hotels breach has led to the UK's ICO proposing a £98 million fine due to using systems with known vulnerabilities.

Certificates
Applications which use a security certificate to create a secure communication channel to protect data in transit will no longer work if your certificate is expired, revoked, invalid or distrusted which means visitors will not be able to access your site. This can cause interruption to your business and as well as loss of reputation/reliability.

Phishing & Malware
The reports can discover if any of your organisation's web pages is being used as part of a phishing attack or hosting malware. If any of your web pages are being used to host phishing and/or malware content they will be immediately blocked by all the major browsers. Those who are able to access the sites will also be exposed to the threats – and spread them further. This can be particularly harmful to reputation and will cause interruption to your business.

Cyber Training

What is the issue?
Your staff are your biggest asset but also your biggest risk. You need to be able to trust them and to do that you need to ensure you give them the tools to empower them to make the right decisions when dealing with electronic data and messages. Cyber security training is the most important thing you can do to protect your staff and your organisation.
Here are some statistics:

- 90% of cyber incidents are caused by human error,
- 71% of attacks use spear phishing,
- 20% of Android users (Only!) use the most up to date software.
- 50% of cyber security professionals have not updated their passwords in the last year

People are predictably unpredictable and sometimes careless. This is not something that any employer can change – but you can educate and change attitudes.

What problems can a cyber training program face?
Historically, cyber security training has been beset by problems from the outset. Some staff will consider themselves IT literate; perhaps conveniently. Without training, most individuals will have

no concept of the risks that confront them in their daily lives. Training has often been considered patronising especially when it refers to the uneducated in a stereotypical 'them and us' manner. Most employees will not (yet) have the experience to enable them to relate to the cyber threats that really do exist. Any and all training has to be relevant and material to those whom it is being delivered. Both lack of confidence and complacency put your business at risk.
Also, employees will often feel that to spend time on training will impact on the time they have to do their actual jobs. They do not see the value of the cyber training courses so flip through the content, answer a few questions and get back to their day without giving it much thought.

Cyber education can also be seen as a tick box exercise by many managers concentrating on targets and deadlines. This attitude evidently trickles down. This sort of innocent apathy might be disastrous for your business.

Making cyber security training relevant and engaging
The key to fighting this apathy is making sure the training content on offer is relevant to the individual rather than just 'the company'. People are more likely to engage with the program if they understand 'what's in it for them"' In order to value the experience it also needs to have an immediacy and be memorable to the recipient. The programs we can provide use humour, videos and interactive content to great effect.
BGi.uk have partnered with several specialist cyber businesses who provide training programs. Each has a different approach to the method of delivery; but the aim is to achieve the same end goal of cyber security awareness. Sometimes quirky but always informative.

Making cyber security training effective
Each program is separated by topic and style. Some are videos which use pop culture and references from the news to draw in the user. Each topic is then separated into modules which are kept minimal in time to avoid cognitive overload and training fatigue. Each concept is distilled down to its components to keep simple. This makes it easier to reinforce and when the user is able to connect the dots in their own mind the concept is more likely to stick.
Users test their skills using real life scenarios which aren't just related to business but their personal cyber behaviours. Once engaged they have the option to learn more with autonomous learning. An area is available for discovery; where new content is produced regularly and linked to the headlines.

Example - A financial controller in a law firm received a call from what seemed to be the firm's bank, explaining that some suspicious wire transfers had been flagged on the business account. The caller insisted that there was an immediate danger of the remaining funds being drained and that they needed a password and a PIN to put a freeze on the account.

The financial controller wanted to avoid any further loss and so confirmed the pin code and password to the caller. It later emerged that this had led to $118,830 being wired to three overseas accounts in nine separate transactions. Because the transactions had seemingly been authorised, no reimbursement was offered by the bank.

With the correct training this sort of social engineering loss is much less likely to occur.

Monitoring the success of the program
The programs we provide also have a fresh approach to monitoring engagement with (and successes of) the program. Assessment is not made solely from correct answers but through completion and engagement with further materials. Rather than using fear of judgement and the accompanying embarrassment or shame; curiosity and engagement become the key motivators for the user.

This is where fresh and current content comes into its own. On the programs we provide there is always something new to learn; keeping user engaged from month to month rather than just once per year.

We can provide you with access to a number of reporting tools to see how different departments or individuals are using the system. From this you can devise an engagement strategy which works for your business. You can then tailor this to suit your requirements for follow up training. Each system uses various nudges for users to refresh their knowledge.

Support
We can also provide support by tracking engagement and highlighting any areas of focus to help you drive further engagement. BGi.uk are also keen to promote this extremely important part of risk management. This enables us to hold meaningful talks with insurers regarding the terms and premiums required for your insurances.
Each program also offers excellent user focused support. Our partners' responsive teams are on hand to help with any issues which might arise. They are also proactive in their approach and will work with you as much as possible to achieve your cyber training goals.

Whatever your company ethos or the environment you would like to foster, whatever you want to achieve with your cyber training program, BGi.uk can help.

Consultancy

Certification
Once you have the broad view of your exposures, and the wider threats, you may want to dig a bit deeper. We work with a number of trusted partners who can provide the consultancy you need to guide you towards meeting your cyber security aims and protocols – and within your budget.
One thing to consider is how you measure up to different standards across industries. Cyber Essentials is a government backed scheme set up to ensure businesses are able to take control of their cyber security. So far only 22,000 certificates have been issued. Why is the take up so low? Although this is at the simpler end of certification it is understandable that many SMEs with no specialist cyber knowledge would be wary of this. This is why we work with companies who can advise you on best practice and help you to achieve this certification with confidence.

If you would like an internationally recognised certification we also have providers who can help with ISO27001. These certifications can give your customers confidence that you take this threat seriously and can be a trusted partner.

Data Consultancy
There are few businesses which do not process data in some way; whether this is sensitive customer data, payments or even your staff records. No matter the nature of the data there is an expectation within law and business that you will take all reasonable steps to ensure its security.
We have an excellent relationship with a data consultancy who specialise in helping you to get the most of your data and understanding the ways in which it can leave you exposed. They can work on mapping your data which will both help you work more efficiently and put you in line with the latest updates in data protection legislation. This means understanding your role as the data controller and fully engaging with your data processors.

This kind of consultancy can help you understand where you fit within a supply chain and consider what you expect from your suppliers. More and more it is becoming usual to expect a reasonable

level of protection and so look at this when discussing your contracts. We are also working with organisations to help streamline this process for you.

Helping you ensure you can demonstrate due diligence.
They can also help with day to day privacy issues which are becoming more prevalent with GDPR. This can include privacy concerns which are reported without merit where investigations must still be carries out and Subject Access Requests. If you do not have a handle on your data dealing with these issues take valuable time and resources from your business. Getting to grips with your data will save you time and money which could end up being invaluable.

Example - A private healthcare clinic was the victim of a cyberattack where patient information had been stolen. Hackers were threatening to post the data on a public website unless they received a ransom payment of $13,220 in Bitcoin.

After an investigation of the insured's network, the forensic specialist was able to advise that data relating to 3,000 patients had been compromised, but it was a database containing names and addresses only – no sensitive medical data had been accessed.

Security Audits
Once you understand your data it is important to make sure you are securing them adequately. We work with a number of organisations who can provide security audits. Allowing an external company to come into your organisation can be intimidating but it allows an unparalleled objectivity
There are two aspects which can be looked at. Your technical security but also your people and how they behave. It is not their aim to be judgemental but to proactively help you to take control of what you can.

They will put your security systems through their paces and provide a detailed report explaining their findings and providing recommendations on improvements. They will be able to let you know how to tighten up your security and help you devise practical policies and procedures to ensure your staff are ready in case of an incident.

Security Consultancy
If you are looking for more ongoing support we can also assist you in finding a company who can provide a regular consultancy with a virtual CISO. For an SME you may not need or want to employ a full time CISO. Through our partners you can pay for a certain number of hours per month in order to help you to come up with a risk management strategy and help you to review this periodically and keep you up to date on best practice within your industry.
Even with the best tech and advice there will always be aspects you cannot control. Our providers can provide pen testing in a number of ways. For your convenience we have providers who can provide on demand pen testing which can be purchased through a simplified portal or through devising bespoke plans suited to you. You can't anticipate how cyber criminals may try to breach your security. 71% of attacks are carried out via spear phishing. These attacks are not the poorly spelled mass mailshots of the past but are much more frequently very convincing and extensively tailored. Information about people is more readily available to cyber criminals, thanks to our social media habits it is not as difficult as you think to figure out what makes someone tick. This is called social engineering.

It is also possible for cyber criminals to intercept email traffic and to impersonate people you may be familiar with through spoofing. They may even be able to refer back to items which were in discussion. This may be an email you were expecting so it is more important than ever to be vigilant. Ethical Hacking is where a cyber security company takes these different approaches to show how

vulnerable you can be. This is one of the best ways to really test your system. The only way to keep up with the bad guys is to inhabit the same space.

Our trusted partners are reputed for their knowledge and professionalism bringing different approaches to your cyber security. Why not talk to us about what you want to achieve.

Incident Response Planning

Things to consider

Even with the best training and security in place it is still likely your business will suffer some sort of breach. In this event it is important to have plans in place to avoid panic and freefall chaos: to ensure things can be resolved as quickly as possible.

You should consider several things before looking at your incident response

- What are your worst case scenarios? For example, how quickly are you likely to start losing revenue? Would loss of IP be potentially fatal?
- Would you need to notify your customers in the event of a breach? Do you need to notify a regulatory body? What are the time frames for this?
- How will you find out what has happened? Do you have your own IT team? Do you outsource this work?
- What aspects do your insurances cover?

The average time a breach remains undiscovered is 175 days – six months! If you are able to identify an incident quickly it can drastically mitigate your losses. Incident response plans provide the first line of defence against breaches and incidents. They also help to establish procedures which mean you nip an incident in the bud; possibly before there is any loss.

Example – A trucking company suffered a ransomware attack where cybercriminals encrypted all of their data files and requested a ransom of $9,920. Hackers had encrypted all of the data that they required to run their operations including routes, logistical information, contacts, and stock levels.

Rather than pay the ransom they set about reconstituting data from paper records and their employees' knowledge of day-to-day operations. This resulted in a large amount of overtime costs and loss of business income that resulted from the extended outage of their systems and the consequential impact on operations.

Preparation

Firstly, you must perform a risk assessment so that you can effectively prioritise your sensitive assets whether this is client data or intellectual property. By doing so you can decide what sort of incidents your plan should focus on. You should consider the systems you use for backing up your data, how frequently you do this, whether this is regularly tested and where this is stored. It is a good idea to keep this off site in case of a physical incident such as fire affecting your premises.
You should then prepare a clear communication plan for your team including documentation which states the roles, accountabilities and processes within the plan so that your team immediately know and understand their responsibilities.

Identification

You should regularly review how your systems are being used and scan for threats so you can detect anything out of the ordinary which could indicate an issue.

At this point, if you work with a cyber consultancy you may be able to contact them for assistance. Similarly, if you a have a cyber policy, you should contact your insurer who may be able to assist either with advice or practical support from forensics or data breach experts.

Containment
Once you identify an incident it is important to contain it to prevent any further damage from occurring. This needs to be done in the short term by taking down affected servers and in the long term by applying fixes that can bring servers back online and to begin recovery.
At this point you need to review the type of data that has been breached and whether you need to notify your client or a regulatory authority, and how you will go about doing so.

Eradication
The cause of the attack must then be identified and dealt with such as the removal of malware. Remedial action should then be taken to prevent similar attacks from happening in future. For example, if a vulnerability was exploited it should be patched or if the cause was a phishing attack staff training should be reviewed.

Recovery
Any affected systems need to be brought back online carefully to ensure another incident does not take place and a process of testing must be implemented to make sure the system is working as normal.
It is important to monitor your systems following an incident as once you have been breached a second attack is more likely.

Lessons Learned
You must then look back on the event and investigate what happened more deeply and reflect on areas where the response was effective and areas that require improvement.

An incident response plan should be complemented by a disaster recovery plan. While an incident response plan focuses on identifying issues and resolving them as quickly as possible, a disaster recovery aims at bringing systems back online, subject to a Recovery Time Objective (RTO). Both are vital to ensure you are prepared in the event of a cyber incident. The most important thing is for this to be communicated to your team and for them to understand their responsibilities and how to respond in the event of an incident.

Cyber Insurers will look at your incident response plan as an indication of how seriously you take the cyber threat. An effective incident response plan is likely to reduce your requirement to claim or ensure the claims costs are kept to a minimum. This is clearly a major concern for insurers and your insurance terms and costs will reflect your attitude to incident response.

Insurance can respond in a number of ways with your incident response plan including assisting with forensic costs and notification costs. It can also respond in other ways to mitigate your loss of revenue including business interruption cover, legal defence costs and public relations costs.

Having a plan such as this is an integral part of cyber-risk management and key in terms of cyber insurance policies. 93% of businesses without a disaster recovery plan go out of business within one year following a serious cyber incident. We work with a number of providers who can help you stay on top of the way your organisation responds to security incidents.

Conclusion

Insurance is not the ultimate solution. It is always best to avoid losses and claims rather rely on insurance which should be considered the last line of defence.

Cyber-risk management need not be expensive or complicated. A few basic steps will raise your basic security signatures to a level where you, your employees and your business will no longer be considered ‘easy pickings’.

BGi.uk can help you understand the way your insurances can work to enhance your risk management strategy. It is not a case of ‘either or’ when it comes to cyber-risk management. We help you to work from a point of best practice with our holistic approach.

At BGi.uk we change the risk by changing the conversation.