ARE YOU PREPARED TO RESPOND TO A CYBER ATTACK?

A Guide to Incident Response for Small Business

Michael Freeman
Southern IT Networks

TABLE OF **CONTENTS**

About
SOUTHERN IT

Michael Freeman started Southern IT Networks Ltd in 2003 and now delivers IT Support and Security solutions for small businesses across the UK, giving them the technology, services, and processes they need to reduce costs and deliver exceptional service. More recently, with a world-class, Security Operations Centre and Help Desk, we not only remotely monitor, manage, secure and backup our clients' IT, but also deliver affordable IT security aimed at the SME.

Until recently, Cyber security at this level was the preserve of the enterprise businesses, but with the ever growing threat of cyber attacks to the SME we decided to do something about it. A Certification body for the UK Governments Cyber Essentials and Cyber Essentials PLUS and also the IASME Governance standard, we put security at the forefront of everything we do for our clients.

This guide started life by Michael putting together an internal and client facing checklist for Incident Response and ended up as what you're reading today.

For more information, visit https://www.SouthernIT.com and follow on LinkedIn / Twitter @SouthernIT

Key Takeaways

FOR SMALL BUSINESS

After reading through this guide you should be able to cover the following areas, don't make this a one time exercise though. Make your preparations and then rehearse and review them on a regular basis.

BE PREPARED

Being prepared is key — knowing what to do (and what not to do) is critical before a cyber event occurs.

CHECKLISTS & PROCESSES

Having standard organisational processes can reduce damage to the company and reduce incident cost.

HAVING A PLAN IS CRITICAL

Communication and collaboration with your team on how to handle the media is critical. You must involve all stakeholders, including any external resources you use.

TRAINING STAFF

Everyone in the organisation needs to be trained and to practice regularly, so it's not foreign when an attack happens. This can be through online and in person training.

General
OVERVIEW

Effective incident response is a complex undertaking. Establishing a successful incident response capability requires substantial planning and resources.

The recommendations/guides in this book are designed to assist small businesses in establishing computer security incident response plans and capabilities, enabling you to handle incidents efficiently and effectively.

You'll likely work with your IT Providers to complete all the requirements of your plan, as I've deliberately left some elements 'technical' because it's imperative you have this conversation with your IT Partner.

Before you start designing your Incident Response Plan, check with your Cyber/IT Insurance providers to see if they have a set process that they require you to follow in the event of an incident. You don't want to inadvertently invalidate any policies you may have in place.

Attacks and Technology have moved on

What you use today to protect yourself from a cyber attack should look quite different to what it would have just 2-3 years ago. Attacks have become much more prevalent and the technology that was once the preserve of enterprises is now affordable to the SME and what we (as IT Partners) provided as a solid security approach 12 – 18 months ago, just doesn't afford you the basic level of protection from the evolving cyber threats.

Security offerings need to improve pro-actively and reactively to maintain the same standard of protection you have come

to expect from your current protection and there is another element to this, shared responsibility.

You need to realise that as well as every piece of technology you have, you also need to invest in your 'Human Firewall' with a programme of regular security awareness training. This is certainly something your IT Partner can assist you with, but is one of those areas that's most definitely a shared responsibility.

But I'm just a small business, the attackers aren't after me

While you may not be an actual target of a cyber-attack, you're more likely to be caught in a volume attack based on extorting money from your business, to the cyber criminals it's just a numbers game.

They know that some people will click a link, send money to a bogus bank account, have weak passwords that can be cracked quickly etc. So, while you may not be targeted explicitly, you are very much at risk. Small businesses are the victims of the majority of today's attacks, and that is because they are often under protected and being under prepared will cost you dearly.

Even so, my data isn't that valuable

This may be so, but in every case we've ever seen it is always more valuable than you think. If you are the target of an attack it's because you have something they want and it's worth the time and effort of them getting it from you.

But, in the majority of these volume-based attacks, the cyber-criminal doesn't want your data, but they know that you cannot work without it and will likely pay to get it back if it's encrypted (locked). This is Ransomware and it's the most common type of attack we see on small businesses today.

A cyber incident wouldn't really affect my business

A lot of small businesses have this same thought. You need a detailed and honest conversation within your business, to discuss the risks and determine the level of risk your business is comfortable with.

What most companies have not factored in, is the chaos of the attack situation:

- Angry clients
- Dealing with Press
- Reputation Damage
- Lost clients
- Loosing valuable files
- The time to restore data and systems
- Having to report breeches to the ICO

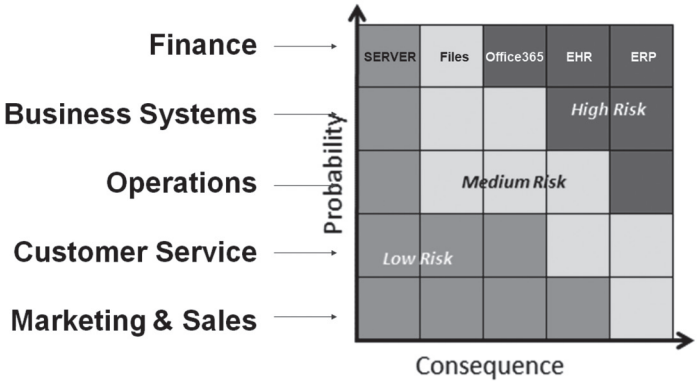
But I've not budgeted for this!

None of us like extra costs, and it's up to you to take these new risks and determine the level of risk your business is comfortable with. If you don't feel expense outweighs the risk than that's your call, at least you have consciously made that decision having evaluated all the options.

The cost of downtime or reputational damage due to a cyber incident is always more than you think. If you want to look at the ways in which you may want to protect your business, take a look at our '15-Ways to defend your business against a cyber attack' resource at SouthernIT.com/15Ways

What Do You Need To **RECOVER?**

This may sound like a simple question, but you'll be amazed at the thought that needs to go in to planning an effective recovery. You're likely not going to be able to recover all your systems at once, so what are the priorities and what systems/applications do the departments need, in order to be functional?



Use a chart like the one above to list each function or department and the services they need to be able to access in order to operate, and grade them by low, medium and high consequence if the service is lost.

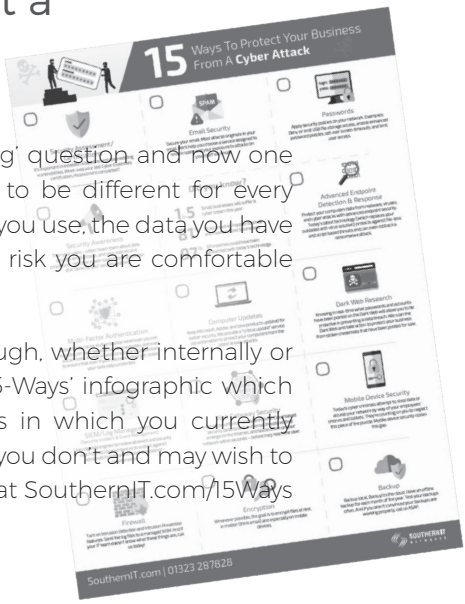
This simple task will give your business recovery priorities that can then be shared with your IT Partner, who can add the technical recovery steps to getting them back up and running in the order that you require. I'll digress a little into backup for a moment, as a next step would be to add to each business function/department, the time in which you wish to recover them within - this is what we term the 'Recovery Time Objective' (RTO).

Now decide how much data you are willing to lose, is it 24 hours worth (once daily backups) or 15 minutes? This is your 'Recovery Point Objective' (RPO).

There is a backup solution for everything, from just backing up your files and folders/cloud applications, to full blown business continuity systems that will have you up and running in minutes and with minimal, if any, data loss.

Depending on the scale of the attack you face, and the amount of data you hold, only the very best Business Continuity plans may be effective. These are important considerations to be made clear to your IT Partner so they can specify your backup solution correctly, then at least you are in charge of deciding the level of risk you're happy to accept, not your IT Partner.

How Do I Protect Against a **CYBER ATTACK?**



This is a 'how long is a piece of string' question and now one that I can answer here. It is going to be different for every business depending on the systems you use, the data you have to protect and how much business risk you are comfortable with.

To get the Conversation started though, whether internally or with your IT Partner, we have our '15-Ways' infographic which can be used to highlight the ways in which you currently protect your systems and those that you don't and may wish to consider. You can find this resource at SouthernIT.com/15Ways

What Is
INCIDENT RESPONSE?

Key Terms & definitions

Event

- Any observable occurrence in a system or network

Adverse Incident

- Any event with negative consequences or impact

Security Incident

A violation or imminent threat of violation to computer security policies, acceptable use policies or standard security practices

Examples of a security incident:

Staff are tricked into opening a "UPS Notice" sent via email that is actually malware; running the tool has infected their computers and established connections to an external host

- An attacker obtains sensitive data and threatens that the details will be released publicly if the organisation does not pay a ransom
- A user exposes sensitive information on social or sharing sites
- An attacker uses a botnet to send high volumes of connections to a web server, causing it to crash (Denial of Service)

What Is
INCIDENT RESPONSE?

The goal of incident response planning is to enable businesses to effectively respond to and manage the events that occur during and after a cyber attack or security incident. From detection to containment and eradication, this all needs careful planning and following any recovery priorities you have identified as a business.

Many businesses have a Business Continuity/IT incident response plan in place to cope with disruption to their organisations. In contrast however, many of these do not include an Incident Response plan for Cyber Security.

Most small businesses are ill-equipped to design and implement an incident response plan. Your IT Company, on the other hand, are generally more practiced in the art of incident response because their businesses depend on it. So involve them deeply in the plan creation, they are the ones that will be carrying out a large part of its implementation.

The Modern
THREAT LANDSCAPE

The number one cyber security threat for business today is ransomware. The National Cyber Security Centre surveys for the last three years show that ransomware attacks are growing in prevalence — and that number is only increasing.

Cyber Security Statistics & Data Points

- 97% report that ransomware is becoming more and more frequent.
- 99% predict that frequency of attacks will continue to increase over the next 2 years.
- 44% of businesses report use of non company owned devices for business work, but no security measures are enforced on them.
- Less than 1 in 3 attacks are reported to the authorities.
- 90% of IT Providers are highly concerned about the ransomware threat in 2017.
- Lack of cyber security training fuels the success of ransomware.
- Less than 20% of businesses train their staff to be Cyber Aware.
- The average attacker is now 'inside' your systems for an average of 197 days before even launching an attack. Detection systems are now key.

It's not a question of IF, but WHEN.

Before An Attack:
PREPARATION

Athletes do it. Sports teams do it. Airline pilots do it. Professional speakers do it. Musicians do it. Event planners do it.

Your Business Needs To Do It.

Proper planning and preparation are essential to successful incident response. When you prepare well, you have a better understanding of what's needed for a particular course of action, but don't keep this in your department - this needs to be known across the whole company and any external partners that will or might be involved.

Being prepared for a cyber security attack can reduce the business risk and potential damage associated with the attack, as well as the difficulty of managing the response and recovery times. Recovery times for those businesses with out a plan, are double that of those that do, and over 60% of businesses that take more than a week to recover, will go bankrupt within 6 months.

Planning leads to awareness. Preparation leads to readiness.

Before An Attack:
PREPARATION

Part of Preparation is Having a Communication Plan

This communication plan is with outside parties. Depending on the scope of the incident, the response team may need to communicate with outside organisations such as:

- Law Enforcement
- ISP's/IT Providers
- Software/Hardware Vendors
- The Media
- Other Incident Response Teams
- Legal and insurance

The key is to develop this plan and strategy **before** you need it.

Communication plans with outside parties should document:

- Who is authorised to communicate with each type of outside party and what can (and cannot) be shared
- When you should hire an outside communication management firm and/or legal firm
- Required staff training and processes for handling the media if/when necessary
- The importance of not revealing sensitive information
- How to handle contact, communication and interactions with authorised team members
- A statement of the current status of an incident, so all interactions are up to date and consistent

Before An Attack:

PREPARATION

Preparation

- **Solid Documentation of your systems**

  This is something your IT Partner is likely doing as part of their contract with you, but they may not know everything about how you use your systems. Work together to ensure you both paint a complete picture on all the systems and processes used.

- **Isolated Backup Systems That are Regularly Tested**

  Your backup systems need to be off-site, most ransomware will also encrypt any local backups attached to your network.

- **Periodic Risk Assessments/Certifications**

  Having a 3rd Party assessment carried out of your technical controls and procedures such as what Cyber Essentials or the IASME Governance standard will give you

- **Cyber 'Drills'**

  Practice makes perfect! Don't just leave that plan on paper, the NCSC have their Exercise in a Box tool-kit that you can use, with 'fake malware' to test your detection and response systems.

- **Work with your IT Partner.**

  Make sure your IT Provider works with you to understand your business requirements and what order to recover systems in. They will be critical in recommending security controls for your business.

- **Malware Prevention at all Levels**

  Traditional Anti-Virus and firewalls just don't cut it anymore. The way we do business has changed massively and the tools we need to defend ourselves have to as well.

- **User Awareness Training for staff**

  You must, must, must!...train all your staff in being Cyber aware. Do they know the warning signs to spot a phishing email? CEO Fraud? Or social engineering attempts? Your Human Firewall may be your last line of defence.

Before An Attack:
PREPARATION

Prep Stage Checklist

- ☐ Schedule a vulnerability assessment
- ☐ Check backup routines (test at least twice monthly)
- ☐ Prevent spam from entering the network
- ☐ Apply security-minded group policies
- ☐ Lock down application data & windows/temp folders
- ☐ Setup Active Directory account lockout policy
- ☐ Increase password complexity requirements
- ☐ Auto-expire inactive accounts after X days
- ☐ Establish unknown USB device policy
- ☐ Setup OS updates and patch management
- ☐ Deploy anti-virus/advanced enpoint security
- ☐ Deploy mobile devices security capabilities
- ☐ Configure web/DNS gateway security
- ☐ Setup/configure logging & SIEM console
- ☐ Test and update firewall rules/engine
- ☐ Review findings from vulnerability scan
- ☐ Close unnecessary ports
- ☐ Close RDP/require VPN for remote access
- ☐ Geo-Block international traffic
- ☐ Set up intrusion prevention/intrusion detection
- ☐ Set up multi-factor authenication/SSO
- ☐ Setup dark web scanning for stolen credentials
- ☐ Setup encryption on mobile devices and email
- ☐ Establish employee security awareness training
- ☐ Confirm details within your cyber insurance policy
- ☐ Review/update existing policies & procedures
- ☐ Verify data owner(s) and emergency processes
- ☐ Improve backup routine as needed
- ☐ Document ALL information in internal systems

During An Attack:
RESPONDING TO CRISIS

Responding to a Ransomware Attack

When data has been stolen or is being held hostage, companies are increasingly caving in and meeting attacker's demands for payment. In reality, however, the best defence is a good offense.

The phone rings and you can't believe what you're hearing on the other end — something has taken over your corporate network and encrypted all your data. Supposedly the only way to get it all back is to pay a significant sum to an anonymous third party. The threat of ransomware is very real today — particularly in the SME market — and is a growing problem both in its volume and significance.

As part of your strategy to mitigate risk and avoid falling victim to ransomware (in addition to the security solutions you're leveraging), you should be setting up regular and consistent backups (along with tested and verified restores).

Another solution is application whitelisting. This involves computing "digital fingerprints" for all programmes, patches, additional services and much more.

During An Attack:
RESPONDING TO CRISIS

Detection & Analysis

Attack Vectors

Familiarise yourself with common attack vectors such as:

- Removable/External media, attrition (brute force methods), web, email, impersonation, improper usage (violation of the acceptable use policies), theft, document responses to unknown or new threat types

Validate the reported incident

(And remember that reports can be inaccurate)

- The first step is to confirm whether a reported ransomware infection is an actual infection. There are cases where a user reports what they think is ransomware, but it turns out to be adware, phishing, or some other virus. Validation is important because it keeps efforts focused on important issues. But if you see a ransomware note demanding payment to unlock files, and your system or files are locked or frozen, then you've been hit.
- Declare an incident
- Assemble the response team
- Take action

During An Attack:

RESPONDING TO CRISIS

Sources and Indications of an Incident

The next step is to determine the scope of the incident, including which networks, applications and systems are impacted and whether the ransomware continues to spread. This is often the role of the IT and security specialists.

Alerts

- IDPSs, SIEMs, Antivirus software,
- File Integrity software,
- Third-party monitoring services

Logs

- Operating System, Service, Application, Network Device,
- Network Flows

People

- People within the organisation
- People from other organisations

During An Attack:
RESPONDING TO CRISIS

Analysis

- Profile Systems
- Understand Normal Behavior
- Create a Log Retention Policy
- Perform Event Correlation
  - You may need to compare logs from differing sources to see the scope of an attack
  - An AV may see an infection on a system and point to a cause
  - The Firewall logs may show the full source and scope of an intrusion
- Keep all Clocks Synchronised
- Use Internet Search Engines for Research
- Run Packet Sniffers & Vulnerability Scans
- Seek Help From IT Professionals

Documentation

- Document All Findings
- Start immediately on suspicion of an incident

During An Attack:
RESPONDING TO CRISIS

Considerations for Containment

- Potential Damage to and theft of resources
- Need for Evidence Preservation (Legal and Insurance)
- Service Availability
- Time and Resources Needed to Implement
- Effectiveness of the Strategy
- Duration of the Solution (Emergency Workaround vs. Permanent Solution)
- Compromised accounts may still have access to the network.

During An Attack:
RESPONDING TO CRISIS

Considerations for Containment

- Deny all international traffic in the firewall, except Ireland (Microsoft O365 runs there!)
- Deny all inbound traffic across RDP or other remote access tools to the client site. If necessary, enable VPN access first then to RDP connection.
- Check all security and system logs for any unusual activity. Note if the logs had been deleted. (If deleted, restore logs from backup)
- Check local (and domain) accounts for any changes or new accounts you weren't expecting to see.
- Reset all passwords to a default password - then share that new password verbally around the office so they can reset their passwords. Don't email it out. And force them to change from the new temporary password you set. If you just force password changes, then there is a chance the threat actor will reset their compromised account and still have access to the network.

During An Attack:
RESPONDING TO CRISIS

Containment Activities

- Isolate Infected Machines
- Do not power down machines unless you have made specific plans for it (autorun commands could cause the spread of threats on boot up)
- Scan all machines with multiple tools
- Lock down firewalls and verify all rules
- Monitor firewall and network logs for additional intrusions

Eradication and Recovery

Investigate

- The investigation starts by preserving evidence. Some machines will need to be returned to service as soon as possible while others might be less critical. Evidence such as log files or system images is taken off the affected machines, along with documentation of serial numbers and asset identifiers.

Eradicate

- The eradication phase removes the ransomware from machines and brings them back into a functioning state. Isolated machines are wiped, and then data is restored from backup to each of the machines after the evidence on the computers has been preserved. In some cases, organisations may decide to remove the ransomware and then restore files that were encrypted by the ransomware without wiping the device first.

- A full machine restoration prevents other ransomware or malware from causing problems on the computer, and it also prevents backdoors or other software that the ransomware might have installed from being used to infect the machine later. For this reason, it is typically recommended that you wipe the device, then restore the operating system and data from backup.

Remediate

- The last step is to remediate the problem that the ransomware exploited in the first place. This is often a user behaviour or training issue, in which case additional awareness training, coaching or simulations can be implemented. In other cases, new technology needs to be put in place. If backups were found to be inadequate, the company would back up more data or back up more often. The ransomware incident should result in some improvement actions that the business can perform to be better prepared for future incidents.

- Rebuild any system that was infected and could not be cleaned

- Any system with activity that looks like a threat and could not be identified should also be wiped and rebuilt

- Maintain forensic data needed by insurance and investigators

- Tighten down the network to restrict the same attack from happening again (once a network is attacked, it is often repeated)

During An Attack:
RESPONDING TO CRISIS

- Restart backup routine ASAP
- Use a phased approach so that remediation steps are prioritised–For a large business this can take weeks or months – Do not rush

Post-incident Activity

- Lessons Learned
  - Debrief and Document Learnings
- Use Data Collected to Improve Response and Prevention
- Determine Evidence Retention for the Incident
  - Prosecution
  - Data Retention
  - Cost

During An Attack:

RESPONDING TO CRISIS

1. What to do Immediately Following a Cyber Attack

- ☐ Call your business insurance company. They will explain their requirements and outline any steps that may need to be taken to protect forensic data or evidence. You want to support—not hinder your ability to collect an insurance claim.

- ☐ Review the companies business continuity or disaster recovery plan, as there may be specific requirements and action items mandated by certain policies.

- ☐ Reiterate the company's rules of disclosure to employees, and to address what should or should not be communicated via public channels like social media, the press, as well as with clients. A standard recommendation is that nothing is permitted to be disclosed until the company releases a formal statement (generally after the facts of the event have been gathered and properly analysed).

- ☐ Back up everything – even encrypted or infected computers to create a recovery path if the containment or remediation steps destroy data (or in the event that decryption fails and a recovery key is discovered after the event has occurred). There are cases where the threat actor releases the decryption key months after an attack has stopped paying dividends.

During An Attack:

RESPONDING TO CRISIS

2. Containment

- ☐ Run an external vulnerability scan from the internet to look for anything unusual (e.g. ports) that shouldn't be open in the firewall
- ☐ Deny all international traffic in the firewall.
- ☐ Deny all inbound traffic across RDP or other remote access tools to the client site. If necessary, enable VPN access first, then RDP across the VPN-protected connection. If possible, unplug your internet connection at the router until you have regained control of the network. You can also unplug all switches on the network to help avoid lateral movement of the threat and isolate segments of the network as you work to contain.
- ☐ Check all security and system logs for any unusual activity.
- ☐ Test your backups, and if possible create a manual set and store them off the network.
- ☐ If you have Dark Web Monitoring, check for stolen credentials on it.

During An Attack:
RESPONDING TO CRISIS

2. Containment (Continued)

- ☐ Check local and domain accounts for any changes, or new accounts you weren't expecting to see. You may use RapidFire Tools to automate this step. Remove or disable any old accounts and verify ones created recently as being expected.
- ☐ If not in place, consider adding DNS protection to prevent further command and control calls to infected websites (bot network)
- ☐ Leverage advanced endpoint protection to help hunt for and isolate the threat, provide additional visibility, and help prevent further spread of the attack.
- ☐ Leverage SIEM Technologies (Security Information and Event Monitoring) to analyse and provide additional visibility into the activity going through the firewall, in Active Directory, and on endpoints.
- ☐ Receive authorisation (in writing, email or text from the insurance provider, before moving to the Remediation Steps. (if applicable)

During An Attack:
RESPONDING TO CRISIS

3. Remediation

Note: Before beginning these steps, unplug the internet connection and either unplug the switches on the network or disconnect all machines (including servers). Consider also removing the gateway IP address from the network temporarily. Some of these steps may not apply depending on the type of network you are running.

- ☐ Clean a domain controller (possibly in safe mode) of the infection.
- ☐ Disable Autorun on all systems on the network using a Group Policy Object (GPO) in Windows.

Note: It is strongly recommended to disable the Autorun feature using Group Policy from the Domain Controller / Centrally.

- ☐ Disable Windows Task Scheduler on all systems on the network.

Note: It is strongly recommended to disable the Windows Task Scheduler using Group Policy from the Domain Controller / centrally.

- ☐ Reset all user passwords to a default password, then share that new password verbally around the office so users can reset their passwords. Do not email it out, and be sure to force users to change from the new temporary password you set. If you only force password changes, then there is a chance the threat actor will reset their compromised account and still have access to the network.
- ☐ Reset all device passwords, including switches, routers, firewalls, VPNs, IDS devices, etc.
- ☐ Bring up one server at a time, clean it, and if it's not a required server shut it down until you have completed cleanup of the network.
- ☐ Bring up one workstation at a time (of the network) and clean as needed. Reboot several times looking for a return of the infection.
- ☐ Check your backups again. You can never have enough good backups.

During An Attack:

RESPONDING TO CRISIS

4. Recovery

- ☐ Restore from clean backups
- ☐ If clean backups do not exist, Southern IT does not advise as to whether you should pay a ransom. That decision is entirely up to the insurance company and the data owners.
- ☐ Scan the network one more time with relevant tools.
- ☐ Once the network is back online, run a new backup job and backup all critical data before allowing users back onto the network. In certain cases this may be a time-consuming effort, but is well worth it vs. running the risk of a second or repeat infection occurring.

5. Debrief

- ☐ Review and document the entire incident
- ☐ Debrief with your response team and IT Provider fully, and work to design and implement a security plan designed for your budget that will help defend against this type of attack in the future.

After An Attack:
MEDIA & PR RESPONSE

In addition to the major costs and risks associated with managing a security incident, the potential damage to brand and reputation (and loss of customer trust) can be equally damaging.

Beyond reputation impact, poorly managed and communicated security incidents can affect employee morale, as well as lead to regulatory pressure and litigation.

Expectations are changing as the frequency and severity of cyber attacks continue to increase. Even organisations with highly sophisticated cyber defense solutions can fall victim to an attack. Businesses should be judged based on how well they manage and respond to an incident, rather than by whether they can prevent one from occurring in the first place. The most well-protected businesses, however, are the ones that can focus on both strategies.

Communicating effectively with all staff and outside parties requires careful planning, as well as an understanding of the unique dynamics cyber security issues that make them different than other crises.

Provided here are several steps you should consider taking now to be prepared to handle a potential incident.

How To Respond:
MEDIA & PUBLIC RELATIONS

What to Say, What Not to Say, and How to Say It

The reporter's priorities are the reporter, editor, rival reporters, readers or viewing/listening audience and (lastly) the source: You.

Before speaking with the media, a spokesperson needs to be well prepared:

- Understand the angle so you know why the interview is important to the reporter and their readers
- Realise how the printed story will impact your company and stakeholders
- Make sure that your company's image and position consistently comes through during every interview

How To Respond:

MEDIA & PUBLIC RELATIONS

Tips For a Successful Interview

- Prepare by rehearsing with your PR team or internal members of your organisation to become more comfortable with the topic and key messages
- Don't assume the reporter is an expert on the topic
- Listen carefully before responding
- Remember that quotes, NOT questions, will appear in the article
- Use clear, simple language without jargon
- Stay on topic with the reporter
- Talk slowly
- Assume everything is "on the record" and being recorded
- Never put the reporter's call on hold
- Vary the inflection and tone of your voice to add variety
- Never say "no comment"
- It's okay to take pauses before you answer; don't be pressured by silence
- Communicate your company's key messages
- Be straightforward; and if you don't know something, be honest and offer to follow up at a later time
- When a reporter presents several questions at once, focus on the question that you want to answer
- Don't speak negatively of any other organisation
- Stick to the facts rather than opinions, and never speculate
- Use anecdotes or real examples when possible
- Summarise at the end
- Be available for fact-checking or to provide more information after the interview
- Don't assume you'll have a chance to review before publication

How To Respond:
MEDIA & PUBLIC RELATIONS

Techniques for Answering Questions

These are designed to help you take control of any interview and create an effective dialogue or two-way conversation, rather than waiting for the reporter's questions which could limit what you're hoping to say.

1. Bridging - this is a technique that allows you to incorporate your key messages into all the answers.

Bridge examples:

- Let's look at it from a broader perspective...
- There is an equally important concern...
- Let's not lose sight of the underlying issue...
- I'd like to tell you about...
- Let me put it this way...
- A story that may help explain...
- That information is proprietary, but what I can tell you is...
- Let me begin by saying...
- What's important here is...
- What I'm talking about is...
- The point is...
- Let's try it from this perspective...
- That brings to mind...
- What all this means is...

2. Hooking - this technique is used to influence the audience's next question and sets the stage for you to deliver a key message.

You say "There are two very important things we must consider when thinking about..."

The reporter asks "And the second?"

The interview will seem incomplete if the reporter doesn't follow up this question. Make your point and expand on it... incorporating your message.

3. Flagging – is a verbal cue that helps reinforce something you want the reporter to remember.

Flagging Examples:

- The most important thing to remember is...
- The take-away message would be...
- If you remember nothing else, please remember two points...

How To Respond:
MEDIA & PUBLIC RELATIONS

Handling Questions - Be Prepared for Standard Questions

- How did this happen?
- What data did they get?
- How have you ensured this doesn't happen again?

What Makes Effective Key Messages

- Deliver key messages that address the issue at hand
- Keep them short and to the point
- Repeat your key messages throughout the interview
- Messaging is not a script; it's a tool

Final Thoughts on Handling a Media Interview

- Remember, no reporter writes a story that includes a list of questions they asked the interviewee. It's your answers that matter, because that's what makes the story.
- One of your key goals is to appear fresh and spontaneous during the interview, not rehearsed or scripted.
- Everything you say to a reporter — whether before, during or after the interview — can affect the story.
- Even if you disagree with a reporter's story about your company, it doesn't mean the reporter hasn't done his/her job.

How To Respond:

MEDIA & PUBLIC RELATIONS

News Travels Fast. The World has Become Much Smaller

- Because of television, radio, the web and the ongoing growth of social media, information travels around the world at lightning speed
- Breaking news will travel across the world in 30 minutes or less

Public Attitude Toward Breaking News has Evolved

- People are often more offended and upset when a company lies about a situation than about the actual situation itself

The Cost of a Poorly Managed Crisis

- Loss of a good reputation and strong brand
- Loss of market value
- Loss of key relationships
- Loss of credibility
- Increased regulation

How To Respond:
MEDIA & PUBLIC RELATIONS

Crisis Communication

COMPANIES THAT CAN:

- Move swiftly
- Speak affirmatively
- Define and lead the public debate

WILL TURN CRISES INTO OPPORTUNITIES

COMPANIES THAT ARE UNABLE TO DO SO WILL END UP:

- Damaged
- Scarred
- Possibly bankrupt or out of business

ALL CRISES CAN BECOME DISASTERS FROM WHICH THERE MAY BE NO RECOVERY OR RETURN

How To Respond:

MEDIA & PUBLIC RELATIONS

During a Crisis: Incident Handling Checklist

- ☐ Do you understand what has happened?
- ☐ Is everyone on your crisis team aware?
- ☐ Do you have holding statements you can use?
- ☐ Are you logging media interest?
- ☐ Other organisations involvement?
- ☐ Identify key external stakeholders and channels to best reach them
- ☐ Are you showing you care?
- ☐ Have you identified your spokesperson(s)?
- ☐ Prepare key messages, Q&A and FAQ - share with colleagues
- ☐ Consider what visuals might be used to support messaging
- ☐ What is being said on social media?
- ☐ Are you communicating internally?
- ☐ What can you learn from the crisis?

Cyber Security:
USEFUL RESOURCES

I have mentioned a few resources in the guide and added a few more below that you may want to consider reviewing.

National Cyber Security Centre (NCSC) resources

Information for Small and Medium sized Organisations - www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations

Small Business Guide - www.ncsc.gov.uk/collection/small-business-guide

Cyber Essentials Certification and Register - www.cyberessentials.ncsc.gov.uk

Exercise in a Box - www.ncsc.gov.uk/information/exercise-in-a-box

Board Toolkit - www.ncsc.gov.uk/collection/board-toolkit

Staff Training Resources

NCSC Infographics - www.ncsc.gov.uk/information/infographics-ncsc

What would a Cyber Attack look like in the real world? - youtu.be/Y1b8865GOHU

Personal & Business Guidance - www.cyberaware.gov.uk

General Awareness Videos

What's your password? - youtu.be/Tvc4JmWI4Ko

Is that email really from your boss? - youtu.be/eLRGG7oyrdA

What is Cyber Essentials - SouthernIT.com/CyberEssentials

Copyright (c) 2019 Southern IT Networks Ltd.

ALL RIGHTS RESERVED.

No part of this publication may be reproduced, stored in retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopy, recording, or otherwise—except for brief quotations in printed reviews, without the prior written permission of the publisher.

Printed in the United Kingdom

Becoming a victim

IS AN IMMINENT REALITY FOR ALL COMPANIES

How an organisation responds to a cyber incident can often spell the difference between failure and success.

The speed at which you identify and mitigate such incidents makes a significant difference in controlling your risks, cost and exposure. Effective Incident Response management can reduce the risk of future incidents occurring, help you detect incidents at an earlier stage and develop a robust defence against attacks, potentially saving your business.

This guide for small businesses will take you through the considerations and steps of the process.