A CIO’S GUIDE TO CYBER SECURITY IMPROVEMENT

ABOUT THIS GUIDE

With the scale and complexity of the cyber security threats organisations face today, it can be challenging to build and implement an effective strategy to measurably improve your cyber security controls - whether you’re an IT leader responsible for 50, 5,000, or 50,000 users.

WHAT YOU’LL LEARN

By combining best practice frameworks and expertise from globally-recognised security leaders, this step-by-step programme guides you through the critical activities to identify your risks, assess your current exposure – and protect your critical assets, with a prioritised, actionable cyber security improvement plan – suitable for both large and small Enterprises.

- **LEARN** how to build a board-level strategy to measurably improve your cyber security.

- **IDENTIFY** your likely attackers – and the overall risk profile of your organisation.

- **DISCOVER** how to prioritise identified risks - and build an effective improvement plan.
THE NIST CYBER SECURITY FRAMEWORK

The National Institute of Standards and Technology cyber security framework (CSF) is recognised by many as an essential resource to transform the security operations, risk management and governance for both public and private organisations.

In this guide, we take a deep dive into the first stages of the framework - IDENTIFY & PROTECT.

It’s important to first understand the risk profile of your business, then set about assessing your current cyber defences – from which you can accelerate your security transformation by building a prioritised action plan.
ABOUT COMTACT LTD.

Established in 2005, Comtact Ltd. is a specialist full-service cyber security provider operating 24/7 from a state-of-the-art Security Operations Centre (SOC) in Northampton, UK – located at the heart of a secure Tier 3 data centre.

SECURITY TO THE CORE

Comtact’s Security Operations Centre combines the very best practice on Cyber prevention and defence, with market-leading intelligence, to ensure we’re always ahead of today’s fast evolving cyber threats.

CYBER DEFENCE CENTRE

Located at the heart of a high security, controlled-access Tier 3 data centre in Northampton, Comtact’s state-of-the-art UK Cyber Defence Centre (SOC) targets, hunts & disrupts hacker behaviour, as part of a multilayered security defence, helping secure some of the UK’s leading organisations.

- Highly experienced UK-based team
- 24/7 ‘eyes on screen’ security operations
- Best-in-class processes & services
- Redundant and secure state-of-the-art facilities
- UK focused, UK staffed, UK governance – on first name terms

ISO27001-accredited

Comtact Ltd. and its operations are ISO27001-accredited
Our Expertise

We offer a full range of specialist cyber security services; always placing the client’s needs at the heart of the solution.

**Assessment**
The first and most important step towards forming an effective defence.
- SECURITY ASSESSMENTS
- PENETRATION TESTING
- VULNERABILITY ASSESSMENT
- PHISHING-AS-A-SERVICE

**Protection**
Protect, manage and secure your perimeter security – the first line of defence.
- ENDPOINT PROTECTION
- NETWORK SECURITY
- MALWARE PREVENTION
- SECURITY PATCHING & CONFIGURATION

**Monitoring**
24/7 ‘eyes on screen’ monitoring to defend and protect your most critical assets.
- 24/7 THREAT MANAGEMENT -AS-A-SERVICE
- 24/7 SECURITY MONITORING
- 24/7 SOC-AS-A-SERVICE

**Cyber Awareness**
User awareness training & assessment, to assist and protect your workforce.
- USER AWARENESS TRAINING
- SOCIAL ENGINEERING

**Security Consultancy**
Call upon the expertise of some of the UK’s leading security authorities.
- CYBER IMPROVEMENT PROGRAMMES
- BEST PRACTICE POLICIES
- DATA SECURITY & USER PRIVILEGES
PROGRAMME OVERVIEW

9 STEPS TO CYBER SECURITY IMPROVEMENT

1. START
Today is no better day to start implementing the core security controls every organisation requires.

2. UNDERSTAND
What’s important for your business to protect? Your data? Intellectual property? Business continuity? Your reputation?

3. KNOW
Who are your likely attackers? What motivates them? What are their objectives?

IDENTIFIED RISK PROFILE

4. EXPOSURE
Knowing your business – and the environment you operate, what are your perceived areas of risk?

5. BENCHMARK
“What is the current state of my security?” Assess and baseline your existing security controls.

RISK EXPOSURE

6. PRIORITISE
Having assessed your cyber security controls, you are now able to prioritise your risks.

7. PLAN
Target improvements, with a prioritised action plan to bridge the gaps in your security.

8. IMPROVE
Turn the plan into action – and demonstrate measurable progress and improvements.

IMPROVED CYBER SECURITY

9. VALIDATE
Evaluate, quantify and confirm the improvements in your security.
IDENTIFY

A high-level ‘macro’ assessment to understand the risks associated with your business and environment, the cyber security threats faced and the likely business impact from an attack.

- What are your most valuable assets?
- Who are your likely attackers?
- What are their motives?
Before you build a comprehensive cyber security improvement programme, begin by implementing the essential set of security controls every business requires. And start today.

On a ‘macro’ level, understand what’s important to your organisation and therefore what’s important to protect. Consider your valuable assets - from customer data and revenue streams, to brand reputation and Intellectual Property.

Know who your likely attackers are. Are attacks likely to be opportunistic, or targeted? What are your attackers’ motives – are they highly motivated? What are their likely objectives? And how/where would they attack?

Demonstrate the appropriate risks your organisation faces. Without knowing your risk profile, you could waste time, effort and money implementing measures to defend against events that are unlikely to occur or won’t have much material impact on your organisation. Likewise, it is possible to underestimate or overlook risks that could cause significant damage.
Before you spend valuable time & resource building a comprehensive cyber security improvement programme, it’s important to act now – to implement the core security controls every organisation requires.

1. **INVENTORY CONTROL OF HARDWARE & SOFTWARE ASSETS.**
   Knowing what hardware or software is on your network gives you the knowledge to prevent unauthorised devices from accessing the network, track changes made to existing devices and control your software inventory.

2. **FIREWALLS & GATEWAYS**
   Not just your main servers, but all internet-enabled devices require adequate protection to police incoming traffic.

3. **SECURE CONFIGURATION**
   Secure configuration means making sure you’ve opted for the best security settings on your devices and software, particularly changing default passwords, ensuring all users use strong and unique passwords, as well as ensuring a robust password reset protocol.

4. **USER ACCESS CONTROL**
   A principle of least privileges ensures you only provide access to what is needed – and restrict access to everything else. In particular, this means careful use of admin rights e.g. removing local admin rights on laptops. It’s also important to correctly administer permission resets.

5. **MALWARE PROTECTION**
   Malware and viruses have become increasingly smart. In additional to ensuring you have effective malware protection on every endpoint device, it is also important users know that inadvertent actions can introduce malware e.g. Email attachments; Phishing emails etc.

6. **PATCH MANAGEMENT**
   Unpatched or out-of-date software is low hanging fruit for a hacker. Ensuring your software is regularly patched will close the open doors. This includes both Microsoft and non-Microsoft software, firmware, as well as business applications e.g. CRM, ERP, web CMS.

7. **CYBER AWARENESS TRAINING**
   Phishing emails, weak passwords, social engineering – Your users are the weakest link in the chain. Whether by inadvertent actions, or manipulation and exploitation by a hacker, employees are an important source of risk to your data security.
By starting with the essentials, you can make rapid and valuable progress towards measurable improvements in your cyber defences – while you take the necessary steps to assess and develop the right cyber security plan for your business.

Although aimed more at SMBs, the UK government-backed Cyber Essentials PLUS scheme provides a good foundation, although doesn’t consider point 7, the risks from your users. Then there are the 6 ‘BASIC’ CIS Critical Security Controls. A US-based organisation – these 6 security controls mirror the Cyber Essentials scheme and is a useful source of reference.

**OUR TOP TIPS**

- Taking swift, actionable steps today to improve your essential security controls avoids the common challenges in almost every organisation of agreeing strategy, developing a detailed plan, agreeing and securing a budget, then actioning the plan – alongside the everyday challenges to keep the business functioning.
- If you do decide to get Cyber Essentials certified, make sure you go for the Cyber Essentials PLUS scheme, which requires an independent assessment.

**REFERENCES**

- [Cyber Essentials](https://cyberessentials.com)
- [CIS top 20 critical security controls](https://www.cisecurity.org/critical-security-controls/)

**USEFUL RESOURCES**

- [Cyber Essentials vs Cyber Essentials PLUS – what’s the difference](https://www.cisecurity.org/critical-security-controls/)
- [What are the 6 CIS BASIC critical security controls](https://www.cisecurity.org/critical-security-controls/)
- [What is a vulnerability scan](https://www.cisecurity.org/critical-security-controls/)
- [Infographic] How to create strong passwords (you can remember!)
A crucial first step in any programme of improvement is to seek to UNDERSTAND and review the threat-prone parts of your business and the risks your organisation faces, at a 'macro' level. Here, we’re not talking about risks like ransomware, or phishing emails, but rather understanding the risks to the inherent value and core functions of your business.

1. What does your business footprint look like?

2. What are your most critical and valuable business assets?

3. What would a hacker find most valuable?
What does your business footprint look like?

LOCATIONS & PEOPLE
What countries do you operate in? How many offices? A few large sites, or disparate? How many remote workers? Are there a lot of temporary workers/contractors? Or perhaps you have extensive 3rd-party relationships in a complex supply chain? What’s the skillset make-up of employees/contractors?

BUSINESS ENVIRONMENT
Is your industry highly regulated? What key compliance standards must you adhere to? Are you a government organisation, or have government contracts?

TOP TIP
SAME BUT DIFFERENT
Two seemingly identical businesses may actually be very different. A business may transact 100% online, direct with consumers. While another may use distribution, via a network of 3rd-party vendors.

It’s important to understand your individual business footprint. Whether you are a bricks and mortar enterprise, operate entirely digitally or a combination between these two extremes, you should consider your full spectrum business presence.

COMPETITIVE ENVIRONMENT
High growth and highly competitive – like an online retailer? Or an established business – perhaps a law firm, or a pharmaceutical company? Market-leader, fast follower, or mid-sized competitor?

DIGITAL FOOTPRINT
What and where are your digital assets? What is your digital trail on social media and the worldwide web? Think about your company information, digital behaviour and electronic reputation as a result of conducting online business. What key digital assets do you have?

PHYSICAL ASSETS
Do you have high value assets, or use high value materials? Control of your physical assets will also rely on digital information to enforce security processes.
IDENTIFY

UNDERSTAND

What’s important to your business?

Information is often the most valuable asset to a business. Physical assets are easy to account for, digital assets are less tangible but are becoming increasingly more valuable. Cyber criminals are highly motivated, highly resourced and operated within an industrialised network, so understanding and accounting for your assets is vital for knowing how to protect them.

Performing regular audits on your physical and digital assets and anything that is essential to core operations will allow you to prioritise how you protect them, rather than applying an expensive and ineffective blanket approach.

TOP TIP

REVENUE
For-profit companies exist to deliver products and/or services which generate revenue and ultimately profit. What is the impact of daily, or hourly revenue being halted or disrupted?

OPERATIONS
The delivery of services is key to many businesses. What is that impact if key services are unavailable? Can you deliver services and/or products on time? Does the operations of 3rd-party suppliers pose a significant risk?

REPUTATION
Your reputation and brand credibility - and the confidence this gives customers.

IP
Your Intellectual Property, or knowledge assets. Trade secrets, copyrighted material, confidential files, product design, R&D information.

DATA
Customer data, a member or suppliers’ database; employee data or the integrity of your business data.

REGULATION
Adherence to regulatory standards.

COMPETITIVE ADVANTAGE
What makes your business unique and different?
UNDERSTAND
What would a hacker find of value?

COMMONLY TARGETED & ATTRACTIVE ASSETS FOR A CYBERCRIMINAL

- Customer data and other Personally Identifiable Information (PII).
- Gaining access to financial services, such as credit card data.
- Digital IP, such as R&D information, source code, engineering data, or details of your supply chain.
- Nation-state intelligence, theft or disruption.
- Identities of influential or high-profile employees.
- Confidential commercial data, such as the names of people with offshore bank accounts.
- Data that likely to cause damage to the business, or individuals such as drug test data of sportspeople or contract details.
- Business disruption, service denial, or holding your data to ransom is also of "value" to the attacker.

Any company or individual employee that uses the internet can be a target for cybercriminals; which is why it is so important to understand how breaches can affect your company, your customers and your employees.

TOP TIP

It’s impossible to prevent cybercrime, you can however proactively anticipate common forms of attack and take necessary precautions to protect against cyber criminals.
IDENTIFY

KNOW

your likely attackers

What’s their typical profile?

Are attacks likely to be opportunistic, or targeted?

What motivates them?

What are their broad objectives?

Having identified the most important things you’re trying to protect – the core value, assets and key business functions of your organisation – it is important to consider who might be attacking you.

Hackers have a lot to gain from a successful breach. By understanding their motivations, personas and objectives, you will have a clear idea of how, where and why they would attack your specific business.
IDENTIFY

KNOW
What are the different cybercriminal personas?

THE OPPORTUNIST HACKER
Anything from a 'script kid' – a novice hacker testing out their skills – to an organised criminal network. Operating indiscriminately, mass distributing malware to probe for vulnerabilities, which they may either exploit themselves, or sell onto other hackers.

Characteristics:
Skilled and proficient, using tried and tested techniques. Snatch and grab raids via website & ecommerce portals, ransomware attacks etc.

MALICIOUS INSIDER
They may be commercially or ideologically motivated. They may be 20% of the threat, but they produce 80% of the damage – it could be an insider controlled via a criminal network, or an ex-employee, sabotaging operations for revenge or profit.

Characteristics:
Insider knowledge provides intimate understanding of processes, so are able to more easily access data files, or circumnavigate security protocols – even to steal physical assets without detection.

TARGETED ATTACK
You may not be a household brand, but you are still likely to be the victim of a targeted attack. Databases of vulnerable organisations are available on the dark web, so it is easy to identify ‘at risk’ organisations. And even small businesses with 10 employees and a £1m turnover could easily pay a “small” ransom of £20k. Invariably, impact/cost of a cyber incident rapidly scales as the size of your organisation increases.

Characteristics:
Skilled, highly resourced and highly motivated, operating within a syndicate. Able to employ a wide toolset of tactics to persistently probe defences, exploit opportunities and slowly extract data – undetected, often over a period of many months.

SOCIO-POLITICAL ‘HACKTIVISTS’
A ‘principled’ idealist, therefore highly motivated by an ideology - whether political, religious, or idealist. Intent of disrupting the corporate agenda, uncovering politically sensitive information, exposing information to inflict reputational damage, or advance their chosen cause.

Characteristics:
A loose, disperse organisational structure, akin to a terrorist cell. Highly varied skill levels, but as we’ve seen, can be highly effective.

NATION STATE HACKERS / TERRORIST NETWORKS
May be working directly for a nation state, or a ‘patriot’, working to advance a nation state’s interests. So, hacking skills could vary from highly advanced and sophisticated, to a simple bedroom activist. Goal may be to steal (learn) state or defence secrets, theft of IP or technologies, of disrupt the operations of Critical National Infrastructure (CNI).

Characteristics:
Highly targeted and highly motivated, but not for financial gain.
IDENTIFY

KNOW

What form could the threat take?

- Theft or unauthorised access of computers, laptops, tablets, mobiles.
- Remote attack on your IT systems or website.
- Attacks to information if you’re a supplier or a third party connected to the business e.g. your hosted services or company bank account.
- Gaining access to information through your staff.

OUR TOP TIPS

1. Every business faces different challenges

Sure, we are all at risk but certain types of business will be more likely to be hit by a certain type of criminal. We’re not all facing the same challenges from the same cyber criminals. The size, profile and nature of your organisation will influence the likelihood of different types of cyber criminals targeting you.

Consider the diversity of these different company examples and what would be most attractive to a potential hacker:

- A mid-sized solicitor.
- A financial services firm.
- A government organisation.
- An online currency exchange business.
- A charity combating extremism.
- A supplier/contractor to the national grid.

2. Don’t think you’re ‘not important or large enough’ to be attacked

Even today, many people believe that since their organisation isn’t a household name, they’re unlikely to be attacked.
The next phase is to baseline and evaluate your existing security controls to allow you to objectively determine your risk exposure; from which you can then prioritise and create an actionable and costed plan – with measurable impact.

Questions:
1. What is the current state of my security?
2. What is my appetite for risk?
3. Is my perception of risk aligned to the reality facing business today?
Assess and measure the potential loss resulting from a specific cyber activity or event. Although risk is an inherent part of doing business, ranking the probability and impact on business can determine how to respond proportionately and appropriately to a level which is consistent with their risk appetite.

<table>
<thead>
<tr>
<th>4</th>
<th>EXPOSURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowing your business – and the environment you operate, what are your perceived areas of risk?</td>
<td></td>
</tr>
<tr>
<td>How much have you historically invested in cyber security?</td>
<td></td>
</tr>
<tr>
<td>How exposed, or ‘at risk’ are your valued assets? What’s the potential business impact?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5</th>
<th>BENCHMARK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline assessment of your existing security controls across your People, Process and Technology to help you answer the question, “What is the current state of my security?”</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6</th>
<th>PRIORITISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Having identified your risks – and objectively assessed the current state of your cyber security controls, you are now able to prioritise (and measurably reduce) your associated risk exposure.</td>
<td></td>
</tr>
</tbody>
</table>
EXPOSURE

What’s your exposure to risk?

It is important to understand your current risk exposure by performing a high-level organisational assessment. Assessing your risk exposure allows you to prioritise corrective actions in an objective, measurable plan.

How exposed / ‘at risk’ are your valued assets?

Your current perception of risk within your organisation may be very different to the actual exposure faced. Consider the organisational factors which will introduce risk:

1. Do you have high profile / high value assets?
2. Do you have a large or disperse workforce?
3. Are there lots of remote/home workers?
4. Do you have lots of 3rd-party contractors or temporary staff?
5. What’s the skill level of your employees?

What’s the potential business impact?

Critically review your assets, business environment (including governance, compliance and market competitiveness) to determine the sources where you are most likely to suffer loss:

1. Disrupted critical processes
2. Lost revenue streams
3. Loss of IP
4. Reputational damage
5. Regulatory fines
EXPOSURE

What’s your exposure to risk?

This is a great exercise to focus your mind on the key risk areas of your business as well as the environment you operate, from which you can then perform a tactical and technical baseline of your security controls.

How much has your organisation historically invested in cyber security?

Today, all types of businesses are reliant on technology. As cyber criminals intensify their attacks, so organisations will need to invest more on protection, detection and response capabilities. How much have you historically invested on cyber security?

What’s the likelihood of attack?

With every passing year, cyber crime is getting worse. Consider the likelihood of an attack from an external threat or the potential of an internal breach by an employees or 3rd-party contractor.

Forrester Research recommends 7-10% of your IT budget should be allocated to cyber security defences.

According to Gartner cyber-security experts, worldwide spending on IT security will jump 8.7% this year, up $124 billion. Compare that to general IT spending, which Gartner expects to grow by only 3.2%.
ASSESS

BENCHMARK

Benchmark your existing security controls

1. Assess the protection safeguards to ensure delivery of critical services.
   - Identity management and access control
   - Awareness & training
   - Data security
   - Information protection, processes & procedures
   - Maintenance
   - Protective technologies

2. Consider your People, Processes & Technologies
   - People
   - Process
   - Technology

3. Using the CIA Triad to assess how Confidentiality, Integrity, or Availability of what you’re trying to protect can be compromised.
   - (C) Confidentiality
   - (I) Integrity
   - (A) Availability

Perform a tactical assessment of your existing security controls – to assess your existing operations and benchmark the security controls around your People, Processes and Technologies.

All of which will help you answer the question, “What is the current state of my security?”

While there are many different types of cyber security assessments in the ‘toolkit’, and different areas of the business to assess, it is important to follow best practice frameworks when assessing your protection safeguards.

‘Avoiding blindspots’

Many organisations make the mistake of starting with the “Benchmark” phase. If you haven’t performed a high-level strategic assessment – to identify what you’re trying to protect, who your likely attackers are, and what is of value to your organisation (and at risk) – it is possible (likely) you will gravitate towards what you already know – namely the most obvious threats.
BENCHMARK
Using the C.I.A. Triad

1. **Confidentiality**
   - Protecting sensitive, private information from unauthorised access.
   - Confidentiality is protecting information from those people unauthorised to view it. It is perhaps the most obvious aspect of the CIA Triad, but also the most targeted/attacked.

2. **Integrity**
   - Data integrity - ensuring data remains accurate and unchanged by unauthorised parties.
   - Ensuring data is an accurate representation of the original secure information.

3. **Availability**
   - Data and information systems are available when required.
   - A DDoS attack (Distributed Denial of Service) is the classic targeted attacks to bring down the respective services - and deny ‘Availability’.

The CIA Triad is a simple, but widely applicable security model; standing for Confidentiality, Integrity and Availability; These three key principles must ALL be guaranteed in any kind of secure system – and thus forms the core data security objectives to maintain.

When performing an assessment, ask yourself: “How could Confidentiality, Integrity, or Availability be affected? Focus on one leg of the triad at a time. If one of these is compromised you’ve lost data security.

**USEFUL RESOURCES**
- What is the CIA Triad?
OUR TOP TIPS

Monitoring your security posture with regular assessments will build a culture of security throughout your organisation. On-going assessment is important because:

1. People are the weakest link – 90% of security breaches are as a result of human error
2. Businesses are embracing cloud and mobile transformation
3. Passing 3rd-party audits are necessary for compliance certifications
4. The cyber threat landscape is ever-changing
5. The earlier you can detect a security breach, the quicker you’re able to contain it and reduce the impact.

BENCHMARK

What’s in the cyber security assessment toolkit?

As you can imagine, there are a wide range of security assessment tools available intended to test your organisation’s security posture. You can conduct security assessments internally or through a third-party – this can be useful if an internal preliminary assessment reveals security gaps, or if you don’t have a dedicated team of IT professionals with expertise in this area. The type of assessment(s) you employ will be governed by your identified objective.

COMMON TYPES OF ASSESSMENT

- Technical assessments
- Interview-based cyber security audit & assessment
- Vulnerability scans
- Penetration testing
- Simulated phishing & Social engineering

USEFUL RESOURCES

- Types of Penetration Tests
- How often should you audit your cyber security?
- Human Hacking – a guide to social engineering
Having identified your risks and objectively assessed the current state of your cyber security controls, you are now able to prioritise your associated risk exposure – from which you can create an actionable plan to measurably reduce your cyber security risks – at an acceptable cost.

For each of your identified risk areas, rate and prioritise your risks as below:

<table>
<thead>
<tr>
<th>LIKELIHOOD</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
<td>Minor</td>
</tr>
<tr>
<td>Minor problem easily handled by normal day to day process</td>
<td>Some disruption possible e.g. damage equal to £500K</td>
</tr>
<tr>
<td>Likely</td>
<td>Moderate</td>
</tr>
<tr>
<td>e.g. between 50% &amp; 90% chance</td>
<td>Significant time/resources required e.g. damage equal to £1 million</td>
</tr>
<tr>
<td>Moderate</td>
<td>Major</td>
</tr>
<tr>
<td>e.g. between 10% &amp; 50% chance</td>
<td>Operations severely damaged e.g. damage equal to £1 million</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>e.g. between 3% &amp; 10% chance</td>
<td>Business survival is at risk e.g. damage equal to £25 million</td>
</tr>
<tr>
<td>Rare</td>
<td></td>
</tr>
<tr>
<td>e.g. &lt; 3% chance</td>
<td></td>
</tr>
</tbody>
</table>

**Likelihood**
- **Almost certain** e.g. >90% chance
- **Likely** e.g. between 50% & 90% chance
- **Moderate** e.g. between 10% & 50% chance
- **Unlikely** e.g. between 3% & 10% chance
- **Rare** e.g. < 3% chance

**Impact**
- **Insignificant**
- **Minor**
- **Moderate**
- **Major**
- **Catastrophic**
TOP TIP

You can’t do everything.

On the face of things, the goal of security seems simple – Protection from any and all cyber attacks.

It isn’t possible to be 100% secure – there isn’t a single organisation on the planet that has the resources to completely defend against every possible type of cyber attack; neither is it a helpful target to aim for.

In situations where it’s impossible to do everything, prioritisation becomes essential.

PRIORITISE

Quantify your risks

Having completed a strategic and tactical assessment of your organisations’ risks, you can be confident you understand your risk exposure – informed, and without blind spots. Risk always remains, but you can now create a plan to mitigate your greatest threats.

What is the practical cost of mitigating the risk?

In the majority of organisations, balance between cost and risk is a central consideration to an organisation’s cyber security strategy. It’s important to estimate the potential loss or cost of recovering from a single incident.

These cost should provide an indication on the amount spent on countermeasures to prevent these threats from materialising. There might be situations in which organisations are willing to accept the risk – either because the likelihood is low or the cost of mitigating the risk is so high. Alternatively, an organisation could transfer the risk by purchasing insurance.
By having prioritised the key improvement areas, the next phase is to create an objective, costed, actionable plan with clear objectives to improve your overall security posture.

**CREATE A PRIORITISED RISK-BASED PLAN**

- Develop a roadmap. Target improvements in a prioritised risk reduction action plan to bridge the gaps in your security.
- Agree the budget requirements of the plan.

**TAKE ACTION & IMPLEMENT IMPROVEMENTS**

- Turn the plan into action and start ticking things off the list.
- Improvements should be prioritised based on impact/severity, probability/cost of impact.

**VALIDATE & MEASURE**

- Evaluate, quantify and confirm the improvement in security.

**IMPROVED CYBER SECURITY**
Turning actions into results will measurably reduce your risk of cyber attack.

Perform periodic assessments to benchmark improvements and reassess areas of improvement – particularly if there have been significant changes in the (internal or external) environment (infrastructure changes, new business acquisitions etc.)

Make cyber security a priority agenda item for the entire organisation – cyber security is a shared responsibility, across multiple functions. The weakest link is too often the human factor.

Cybersecurity can be a competitive advantage – customers, partners and even employees will increasingly choose a company with a better security track record.
TAKE THE NEXT STEP

SPECIALIST CYBER SECURITY SERVICES

Your own ‘full service’ security operations team, fully resourced and expertly supported – 24/7, out of hours, or ‘on-demand’.

24x7x365 SUPPORT

Comtact has a multi-skilled, three-tiered professional support, providing 1st line and 2nd line support operated from our 24x7x365 high security Tier 3 data centre.

Comtact Ltd.
Devonshire House, Bourne Business Park, 5 Dashwood Lang Road, Weybridge KT15 2NY
Tel: 03452 75 75 75
Email: enquiries@comtact.co.uk

© Copyright Comtact Limited 2019

www.comtact.co.uk

Comtact-Ltd
@comtact_ltd