BCS365®

UNDERSTANDING CYBER INSURANCE

to maximize your safety net

The pitfalls of the changing world of cyber insurance can be difficult to navigate alone. **BCS365 can help to make sure your business is protected.**

BCS365®

TABLE OF CONTENTS

TOPICS + DISCUSSIONS

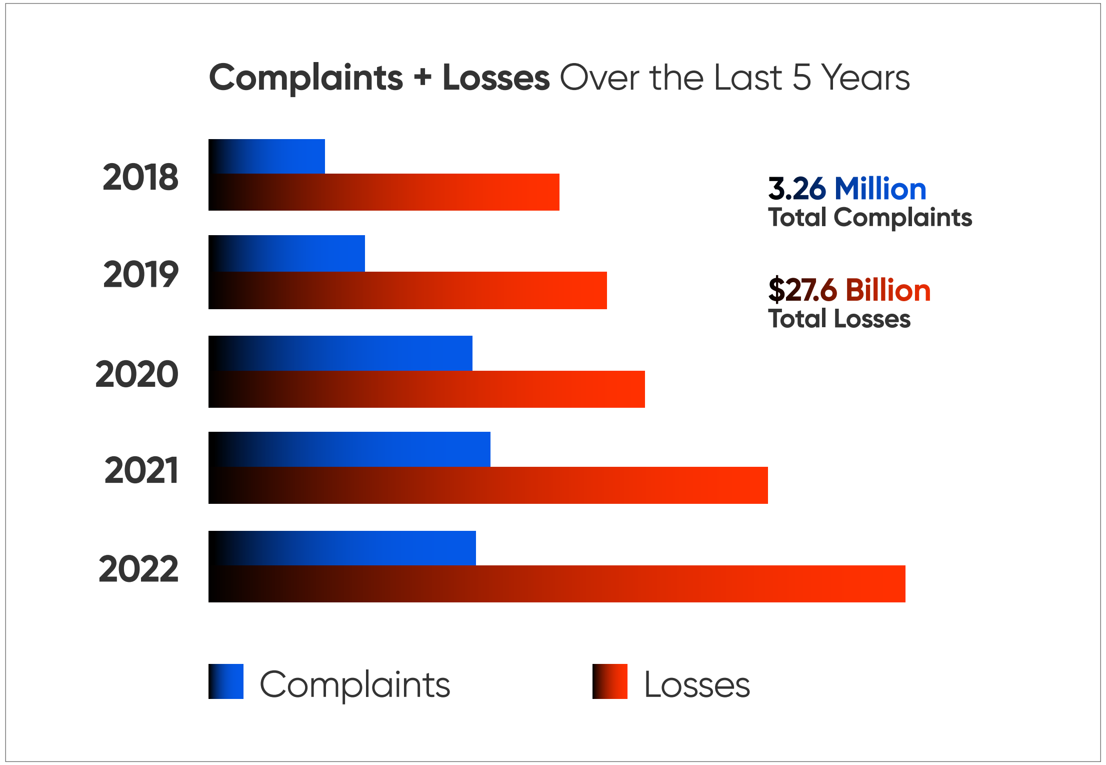
BCS365

INTRODUCTION
TO CYBER INSURANCE

There has long been a culture of complacency when it comes to Cybersecurity within the private sector, especially among small to mid-sized businesses. this is perfectly understandable given that headlines often feature distant corporate giants like Uber, WhatsApp, and Twitter, giving a perception that Cybercriminals are only interested in creating mayhem and embarrassment for brands that are otherwise considered "too big to fall".

Cybercrime statistics, however, paint a different and very costly reality.

In 2022, the FBI's Internet Crime Complaints Center (IC3) received 800,944 reports of malicious online activity, **which translated to a more than $10.2 billion in financial losses**. While this is welcome 5% decrease on the number of incident reports from 2021, the monteary impact has grown by an alarmingly high $3.3 billion - a sharp 48% increase in one year alone.



Researchers at Barracuda Networks analyzed millions of emails and discovered that...

An employee of a small business of fewer than 100 employees will experience **350% more attacks** (such as social engineering through phishing) than an employee of a larger enterprise.

Despite this growing and increasingly apparent risk, many smaller businesses remain unconcerned about the costly and disruptive threats they face. According to survey data compiled by CNBC and SurveyMonkey in the last quarter of 2022, 63% of small business owners express no concern that their business will fall prey to a cyber-attack in the next 12 months, with only 4% citing Cybersecurity as the biggest risk facing their business. This apathy exists despite evidence suggesting SMBs are often ill-prepared to handle the fallout from cyberattacks.

With chilling data form the insurance group, Hiscox, reporting an increase to as many as **one in five businesses** reaching near insolvency as the ultimate impact of becoming victim to cybercrime.

This culture of complacency is often reflected in a lack of corporate policies and measures designed to counter cyber threats.

Faced with constrained IT budgets, staffing challenges and poor awareness of the threat landscape, it's not surprising to discover that **only 14% of SMBs have adequate cyber defense measures in place** according to Accenture's Cost and Cybercrime study. Updated in February 2023, another study conducted by digital.com found that 51% of small businesses had no Cybersecurity measure in place at all.

Why should SMBs bother to tackle threats when they have cyber insurance? They'll take care of any of the fallout, right?

Wrong.

THE GROWING NEED

FOR CYBER INSURANCE

The cyber insurance sector is growing. According to Fortune Business insights, **the global cyber insurance market was around $7 billion in 2020 and is expected to grow to over $60 billion in 2029**. Survey data suggests that around a quarter of small businesses have cyber insurance, with almost half of adopters taking out a policy in response to an attack.

Acting as a “last line of defense” following a cyber-related breach, cyber insurance is designed to indemnify against financial loss and damage, including claims made and litigation pursued by affected third parties. Cybersecurity experts expect cyber insurance to become as common as business insurance this decade but will warn that it is no substitute for taking a holistic, systematic and dilligent approach to cybersecurity. To this very point, regulators globally move to increase the pressure placed upon businesses by taking far more of a stick than carrot approach to incentivize comprehensive data privacy actions are addressed.

NAVIGATING
THE DATA PROTECTION LANDSCAPE

There is growing awareness globally of the value of personal data and a trend towards giving data subjects greater control in terms of how their information is handled, processed and stored.

The European Union's GDPR (General Data Protection Regulation) published in 2016, closely followed by California's CCPA (California Consumer Privacy Act) in 2020 [along with Virginia, Colorado, Utah and Connecticut following suit more recently], have arguably sparked a paradigm shift in relation to attitudes towards data privacy and protection, leading some to speculate that similar federal legislation across the United States could be a matter of when, not if.

A key element of the EU's GDPR regulatory enforcement is **a penalty structure that could impose fines of up to €20 million, or 4% of global annual revenue (whichever is higher) for non-compliance**. While in the US there is no overarching data protection legislation, a growing number of individual states now have some form of data protection law, with some coming relatively close to the provisions of the GDPR. Each of these data protection regimes carries its own penalty scheme, creating a complex patchwork of compliance obstacles for businesses to navigate that operate on an interstate or national scale, in addition to industry-specific, penalty carrying legistation such as HIPPA.

Faced with this endlessly complex and ever-evolving regulatory minefield, it is understandable why an exponentially large number of companies are neglecting to take preventative measures, and instead rely blindly upon their only reactionary failsafe, cyber insurance.

THE SHIFTING THREAT LANDSCAPE

AND IT'S EFFECT ON CYBER INSURANCE

In 2015, cybercrime inflicted $3 trillion worth of damage on the global economy. By the end of 2021, that figure had risen to $6.9 trillion, and according to Cybersecurity Ventures, the global cost of cybercrime could reach $10.5 trillion in 2025.

So, why are cyberbreaches becoming more costly?

GLOBAL CYBERCRIME DAMAGE COSTS:

$6 Trillion USD/year

$500 Billion/month

$115.4 Billion/week

$16.4 Billion/day

$684.9 Million/hour

$11.4 Million/minute

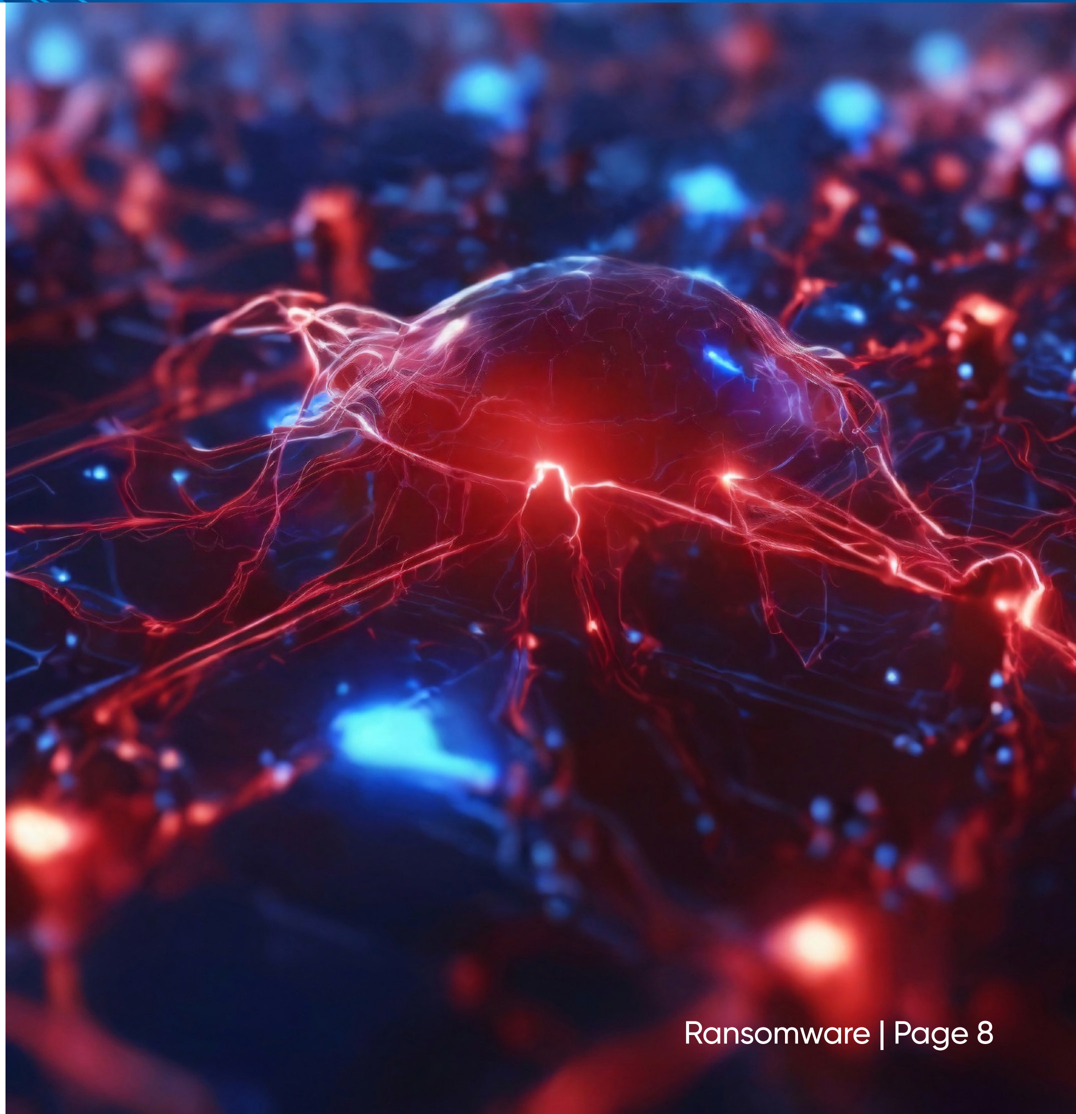
$190,000/second

RANSOMWARE

ONE OF THE MOST PERNICIOUS CYBER THREATS

Featured in around a quarter of all data breaches, **ransomawre is considered one of the most pernicious cyber threats**, with the average attack costing $4.54 million according to IBM's data breach report.

Ransomware has surged in recent years, attributable largely to the entry of elite cybercrime groups into the ransomware sphere. While in the past ransomware attacks were often indiscriminate, the late 2010's saw a distinct shift towards corporate targets, with businesses accounting for 81% of ransomware victims in 2018. Recent years have also seen significant growth in the "ransomware-as-a-service" market, an approach that has allowed cybercriminals to spread risk and upscale their operations by using growing numbers of paid unskilled affiliates to execute attacks on a greater scale.



EXPANDED ATTACK SURFACE

MORE OPPORTUNITIES THAN EVER BEFORE

Criminals operate wherever there are victims to exploit and assets to steal. With more and more business activities being conducted in the digital realm and the total number of global internet users continuing to increase, the criminals have simply moved online to capitalize on a greater number of opportunities, resulting in a corresponding rise in attack volume.

Other factors, such as the growth in network-connected IoT devices and the shift to remote working have further broadened the attack surface, giving cybercriminals a greater number of entry points through which to launch attacks.

PHISHING

Phishing attacks are by far the most commonly encountered cyber threat, accountable for more than 80% of reported security incidents. They seem to be getting more common, too.

Barracuda Networks reported that over 500,000 Microsoft 365 accounts have been breached, along with one in five organizations reporting an account compromise. While once associated with rudimentary tactics and crude deception, phishing scammers have become more sophisticated in recent years, making increased use of BEC (Business Email Compromise) to target high-value victims and using AI tools gather background victims on targets. According to IBM's cost of data breach report, the average cost of a phishing related breach rose from $4.24 million in 2021 to $4.35 million in 2022.

GDPR

The implementation of GDPR in 2018 saw an unprecedented number of organizations fall under the scope of stringent data protection legislation, with actionable penalties administered for non-compliance.

These penalties further increased the overall cost of cybercrime, with high-profile cases (such as Meta's $275 million fine in 2022) reaching mainstream newsfeeds.

COVID-19

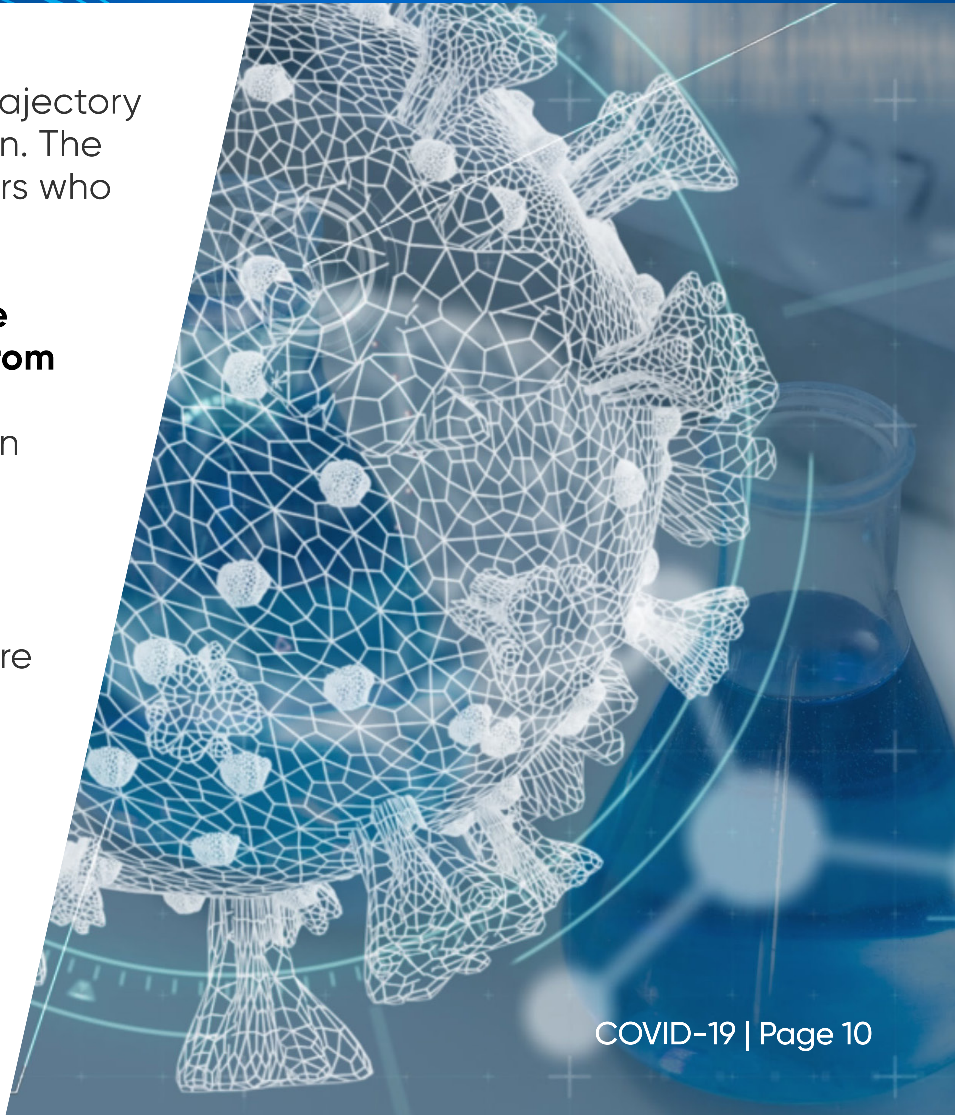
AND THE LINGERING EFFECTS

While cyber threats such as phishing and ransomware were already on an upward trajectory before the pandemic, there is no doubt that COVID-19 has exacerbated the situation. The shift to working from home saw cybercriminals focus their attention on remote workers who were often seen as soft targets.

Barracuda Networks' research noted a **600% increase in phishing attacks during the first few months of the pandemic, with 91% of all cyberattacks in 2020 originating from phishing emails**. These attacks often exploited COVID-related fears, which phishing scammers frequently impersonating health authorities to coerce sensitive information from targets.

In response to this changeing threat landscape, cyber insurance providers have reinvented their offering to recuce the level of risk exposure they face. For insurance customers, these changes are manifesting in two key ways: higher premiums and more stringent qualifying criteria for obtaining cover.

Between 2019 and 2022, cyber insurance premiums have risen by 94%. While once viewed as a low-risk insurance sector, recent years have seen significant increases in both the frequency and magnitude of cyber insurance claims, necessitating this sharp rise in premiums in order for the sector to remain viable.



CYBER INSURANCE

IS DEMANDING A MATURE CYBERSECURITY POSTURE

In addition to the rising cost of cyberattacks, insurers are also mindful of the increasingly onerous data protection landscape businesses find themselves operating within. These two concerns have prompted insurers to introduce a raft of new qualifying criteria for cyber insurance applicants, with minimum standards covering a range of cybersecurity measures.

Evidence of staff security training, regular vulnerability scans and a system log monitoring will continue to be required. Additionally, insurance applicants are expedcted to demonstrate endpoint detection and response (EDR) capabilities and exceed minimum standards in the use of secure authentication measures such as multi-factor authentication (MFA).

Meeting the requirements of a cyber insurance policy is no silver bullet when it comes to maturing your cybersecurity posture, but it enforces certain requirements alongside a wider package of measures and controls ina way that helps reinforce your cybersecurity strategy.

MULTI-FACTOR
AUTHENTICATION

Requiring users to submit multiple pieces of identifying information in order to gain access to a corporate resource, MFA has become a baseline standard to businesses looking to access cyber insurance.

The use of pin numbers, biometric identifiers, physical tokens or codes sent by SMS, in addition to an account password, are some of the most common forms of MFA.

SECURITY AWARENESS

TRAINING + TESTING

Insurers often seek evidence of ongoing and comprehensive security awareness training and testing. Training should educate employees on both emerging and established cyber threats and seek to instill a culture of cyber vigilance in the organization. Employees should know what to do when a suspected threat is encountered, with written policies that instruct on the basis of best practice.

Cybersecurity aptitude can be tested in various ways, with one of the most valuable exercises being the use of mock phishing campaigns. These simulate phishing attacks by mirroring the scenarios and coercive tactics used by real phishing scammers in order to gauge the ability of employees.

MULTIPLE BACKUPS

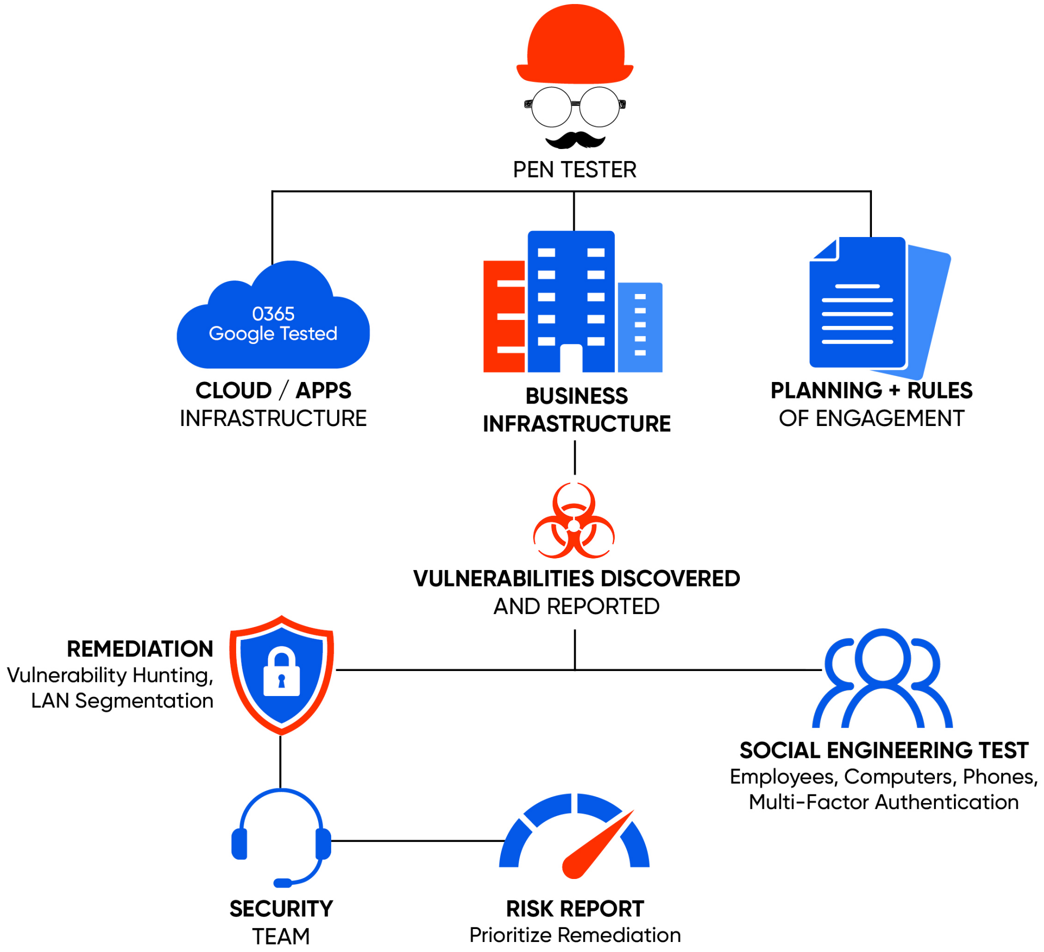
It's not uncommon for small businesses to operate a single data backup, often believing that this is sufficient protection against cyberattacks. In order to obtain cyber insurance, however, organizations are required to establish multiple data backups featuring several storage media and geo-redundancy (data backed up to at least one other secondary location). This strategy reduces risk exposure and aids recoverability in the event that one location is fully compromised.

MANAGED DETECTION + RESPONSE (MDR)

The term "managed detection and response" refers to an organization's capabilities in relation to spotting and neutralizing security threats as they appear in real-time. Using extended detection and response tools (XDR), a managed detection and response team can spot and take action against known threat signatures and anomalous behavior across endpoint devices, networks, identities, clouds and more. A bonus of MDR is the ability to gather and analyze security incident data in order to inform ongoing security posture enhancements.

VULNERABILITY MANAGEMENT

DETECT, CLASSIFY + REPAIR



No system, network or application is infallible. Cybercriminals know this and are constantly on the lookout for weaknesses they can exploit in order to gain access to sensitive data. In order to stay one step ahead of the bad actors, organizations should implement a vulnerability management program that aims to detect, classify and repair vulnerabilities before hackers have the chance to exploit them, thus reducing overall risk exposure.

A key component to vulnerability management, and often a criteria for obtaining cyber insurance, is vulnerability scanning. Insurers typically require applicants to perform regular vulnerability scans as part of an active and all-encompassing vulnerability management strategy in order to qualify for cover.

YOUR CYBERSECURITY OBLIGATIONS

WHAT DO REGULATORS SAY?

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPPA)
Organizations that fall under the scope of HIPPA are required to implement appropriate administrative, physical and technical safeguards to maintain the ongoing confidentiality, integrity and availability of electronic protected health information (e-PHI).

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)
The CMMC is a standard for cybersecurity that applies to all contractors who provide services to the Department of Defense and handle sensitive information. The guidelines for CMMC have been established in the Defense Federal Acquisition Regulation Supplement (DFARS) and Procedures Guidance and Information (PGI).

The requirements outlined in these federally mandated guidelines are exceedingly stringent. Companies must undergo a 110-point assessment, develop and action plan, report their scores, prepare for potential audits, and ensure that their subcontractors and other organizations in the supply chain are CMMC compliant as well.

YOUR CYBERSECURITY OBLIGATIONS

WHAT DO REGULATORS SAY?

THE AMERICAN BAR ASSOCIATION

Law firms are highly susceptible to cyberattacks due to the sensitive information they frequently store on behalf of their clients, including financial records and personal data. The American Bar Association's Model Rules of Professional Conduct stipulate that attorneys must "make reasonable efforts to prevent the inadvertant or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

Moreover, law firms are subject to state-specific regulations that may differ from one state to the next. In California, for instance, law firms are required to comply with the California Consumer Privacy Act (CCPA).

GENERAL DATA PROTECTION REGULATION (GDPR)

Organizations handling personally identifiable information (PII) under the provisions of the EU's GDPR are required to adhere to the legislation's security principle, which states:

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement and appropriate technical and organizational measures to ensure a level of security appropriate to the risk."

Cybersecurity is no single-fix action, and while cyber insurance can offer peace of mind, it should never be viewed as a substitute for a proactive, dilligent and comprehensive approach to data protection. Your goal an an organization should be to mitigate against the cyber risks you face and reduce your exposure to these risks as much as is feasibly possible. So how should you go about doing that?

Let’s consider some of the ways organizational cyber risk can be managed as recommended by leading Cybersecurity bodies.

ISO27001

Published by the International Organization for Standardization and the International Electrotechnical Commission, ISO27001 is the leading global standard pertaining to information security management, featuring detailed guidance on how organizations should develop a robust and comprehensive information security management system (ISMS). The standard’s core aim is to provide a structured framework designed to protect the confidentiality, integrity and availability of an organization’s information assets.

Contained within ISO27001 are a range of perscribed controls that organizations should exlore in order to protect information and manage cyber risk. the standard divides these in to 4 main categores: technical controls, physical controls, administrative controls, and operational controls.

CERTIFIED
ISO
27001:2013
COMPANY

ISO 27001

PERSCRIBED CONTROLS

1 **TECHNICAL CONTROLS**
Technical controls in the form of both hardware and software are recommended to protect data from misuse, unauthorized intrusion and malicious or accidental deletion or modification. Technical solutions advocated include firewalls, anti-virus software and threat detection and response capabilities.

2 **PHYSICAL CONTROLS**
Physical controls refer to measures that protect stored information from physical threats such as theft, environmental degradation or unauthorized intrusion into a premisis by a malicious actor. Some of the recommended controls include CCTV, secure storage, building access controls and temperature and humidity monitoring.

3 **ADMINISTRATIVE CONTROLS**
Administrative controls refer to organization-level measures designed to minimize information security risks through planning, policy, procedure and guidance. Examples of administrative controls include the establishment of information security policies, risk assessments, security training programs, business continuity/disaster recovery planning, and best practice guidance.

4 **OPERATIONAL CONTROLS**
Operational controls consider the ways information security risks can be managed as data passes through an organization’s daily workflows and processes. These controls consider measures such as access management, data backup solutions, data control mechanisms and network maintenance, with procedures and processes recommended relating to each.

NIST CYBERSECURITY FRAMEWORK

Developed by the US National Institute for Standards and Technology, the NIST cybersecurity framework is a package of guidance, standards and best practices designed to help organizations manage their cybersecurity risks.

The process encourages organizations to assess the risks they face, examine the cybersecurity activities currently in place and consider the steps that need to be taken to migrate towards an optimized cybersecurity posture.

The framework divides its material into five key cybersecurity objectives or "functions": Identify, protect, detect, respond, recover. Contained within these functional areas are around 100 security controls that interested organizations are advised to consider. We have outlined some of the most influential controls here.

NIST CYBERSECURITY

FRAMEWORK

1 Access Risk Before Applying Controls

The framework recommends a risk-based approach to cybersecurity, wher the mitigation measures used are commensurate to the risks faced.

2 Deploy Rigorous Identity + Access Controls

Apply user privileges on a strictly as necessary basis and use elevated authentication measures such as MFA (multi-factor authentication) to prevent unauthorized access to sensitive information and systems.

3 Establish Network Monitoring and Threat Detection Capabilities

Install the capacity to monitor networks and systems for unusual activity or anomalous user behavior that might indicate malicious or unsanctioned actions. React to security incidents in a swift manner to limit the potential for data compromise.

4 Train and Educate Staff

Educate staff on cybersecurity best practice and make employees aware of the most common cyber threats and how to spot them, particularly social engineering attacks such as phishing.

5 Perform Regular Data Backups and Institute a Disaster Recovery Plan

Execute regular, comprehensive data backups covering all critical information and develop a sound disaster recovery plan to ensure this data can easily be recovered following a cyber breach event.

6 Manage Vulnerabilities

Conduct regular vulnerability scans and penetration test exercises to highlight weaknesses in systems and networks with a view to performing repairs.

7 Maintain Data Confidentiality

Use encryption and data control mechanisms to maintain the integrity and confidentiality of sensitive data.

8 Test Cyber Preparedness

Draw up plans for responding to a number of possible cyber breach events and conduct simulation exercises to test ongoing readiness.

CYBER ESSENTIALS
IN THE UK

Developed by the UK's National Cybersecurity Centre (NCSC) and launched in 2014, Cyber Essentials is a government-backed certification scheme designed to help organizations across all sectors develop robust foundational cybersecurity measures.

Although certification only applies to UK companies, the scheme features useful, actionable guidance that is relevant to organizations worldwide, and the scheme has been used as a template for similar programs around the world including CyberSecure Canada.

At the scheme's center are five key technical controls which when correctly utilized are thought to protect against roughly 80% of the most commonly encountered cyberattacks: firewall protections, secure configuration, access controls, malware protection, and patch management.

CYBER ESSENTIALS

TECHNICAL CONTROLS

FIREWALL PROTECTIONS

The scheme instructs organizations to deploy firewall protections covering all internet-connected devices. Network boundary firewalls deployed using dedicated firewall appliances or configured at router level should be used to give network-wide protections, and software firewalls should be installed to protect remote devices intended for use outside the organizational network. Firewall rules should be regularly reviewed and maintained.

SECURE CONFIGURATION

The scheme promotes the application of security-optimal settings across all devices and software. Standard settings and default passwords should be reviewed and changed where appropriate to improve security posture, and redundant or unnecessary software programs should be removed to reduce attack opportunities available to cybercriminals.

ACCESS CONTROLS

Cyber best practices require organizations to have robust procedures and measures in place to manage access to corporate resources and authenticate the identities of those seeking access. Multi-factor authentication should be used where available, and strictly enforced password policies should be established to promote password management best practice. User accounts should be disabled and removed when no longer required, and admin privileges should be hosted on dedicated accounts to reduce risk. Extend access privileges to users on a time-limited basis where this is viable.

CYBER ESSENTIALS

TECHNICAL CONTROLS

MALWARE PROTECTION

A number of strategies for reducing the risks associated with malware are promoted. Organizations are required to adopt at least one of these in order to comply with the requirements of the scheme. Suggested measures include installing and activating antivirus software across all endpoint devices, creating and enforcing a “whitelist” of approved applications and using “sandboxing” to execute applicatoins from untrusted sources.

PATCH MANAGEMENT

Organizations are required to apply software updates in a timely manner across all devices, covering both operating systems and installed apps and programs. Auto-update features should be activated where available and unsupported devices or programs should cease to be used.

ABOUT BCS365
AND BARRACUDA MSP

ABOUT BCS365

BCS365 is an information technology solutions provider offering end-to-end managed solutions for clients worldwide. We know you have countless options for providers to manage your IT. BCS365 is committed to delivering 24/7/365 support with U.S.-based experts who are passionate about technology and service excellence.

BCS365 was founded in 2013 and has offices across the U.S. and in the U.K. The company is headquartered in Rockland, MA. We offer a full suite of services including managed IT, security, cloud, and DevOps to clients from all industries including life sciences, manufacturing, finance, and more. Our service team understands that IT support isn't something you just need 8-5, Monday – Friday. You need an always-on team you can count on. **We've got you covered.**

www.BCS365.com

ABOUT BARRACUDA MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP's partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business.

www.barracudamsp.com

BCS365®

1050 Hingham St
Rockland, MA 02370
T (781) 871-0700
F (800) 993-1547
BCS365.com