BRADY.

Brady Cyber Security Strategy

Cybercrime across all industries is on the rise. We recognise your need to have the highest confidence in our ability monitor constantly evolving threats and maintain the confidentiality, integrity and availability of your sensitive information.

We have developed a comprehensive cyber security strategy to give you peace of mind that your Brady applications are underpinned by highly robust security procedures.

Key Priorities

Zero Trust

We ensure that network security is maintained through the implementation of a 'Zero Trust' policy when accessing IT resources.

Defense in Depth

We remove the reliance on perimeter security devices and implement layers of security through the organisation to ensure that IT assets are protected wherever they are at risk.

Shift Left Approach

We conduct the security testing phase early in the product development stage well before going into production.

ISO-27001

We are working towards achieving ISO2700-1 certification to demonstrate our commitment to maintaining confidentiality, integrity and availability of sensitive customer and staff information to the highest of industry standards.

Threats Managed

Attack vectors are constantly evolving. We regularly monitor the cyber security landscape and track trends.
The current major cybercrime threats to your business are from:

Insiders

Hacking

Phishing / Smishing / Social Engineering

Malware

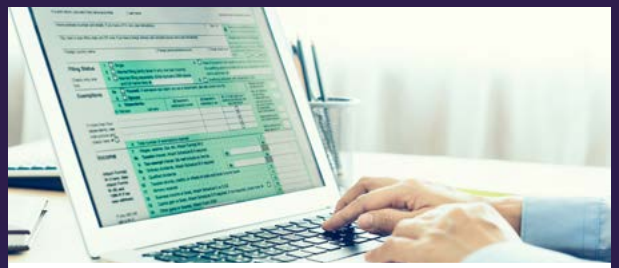
Distributed Denial of Service (DDoS)

Governance

We implement procedures based on best practices to prevent an attack and minimise the impact of a successful attack on your infrastructure and information assets. All Brady staff are clear on their roles and responsibilities in this regard through security awareness training.

Roles and Responsibilities

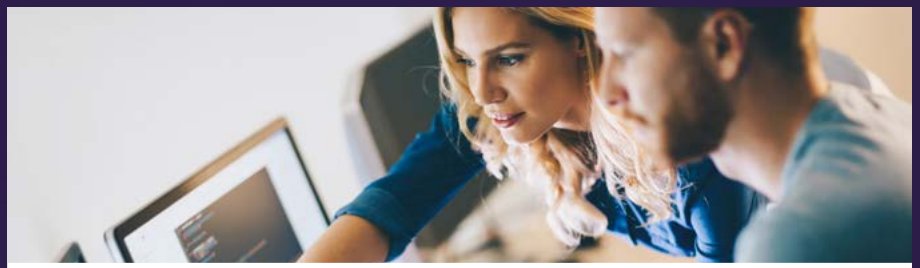
Compliance Working Group (CWG)
The CWG provides specialist advice relating to information management and best practices. The group coordinates the development and implementation of policies and procedures as well as security incident responses. The CWG regularly updates the board.



Asset Owners

All information assets are assigned to owners. Asset Owners are responsible for:

- Updating details on the asset register and identifying correct classification levels for information they are responsible for
- Authorising access to information assets on a 'needs to know' basis, ensuring access is reviewed frequently
- Defining and implementing appropriate safeguards to ensure the confidentiality, integrity and availability of any information asset owned by them



Data Consumers / End Users

Employees, third parties and contractors are authorised by the appropriate asset owners to access information and use the safeguards established by the asset owner. The users are bound by the organisation's acceptable usage policy.

Strategic Awareness

We include cyber security as a risk item on Brady's corporate risk register. This register is supported by a risk treatment plan to identify the remedial actions required to mitigate the cyber security risk. The risk register and treatment plan are reviewed regularly by the internal audit team and the board.

We undertake regular vulnerability testing of all IT infrastructure and implement a planned programme of staff awareness exercises.

We will update our customers on major milestones reached as we work towards achieving ISO-27001 accreditation.

The Strategy

Our cyber security strategy is based on the '10 Steps to Cyber Security' framework produced by the National Cyber Security Centre (https://www.ncsc.gov.uk/collection/10-steps)

By adopting this approach, we will have a strong foundation on which to deliver ISO-27001 and ensure that we operate to the highest of standards to meet our customers' expectations.

Risk Management

Home and Mobile Working

Engagement & Training

Removable Media Controls

Asset Management

Supply Chain Attack

Architecture & Configuration

Vulnerability Management

Incident Management

Identity and Access Management

Logging and Monitoring

Data Security

Risk Management

Taking risks is an everyday part of doing business. We are managing this on a daily basis by:

- Establishing a risk framework
- Identifying the risks
- Analysing the risks
- Evaluating the risks
- Deciding what to do with the risks (avoid, change, share or carry on)

Cyber risk is a priority for our board, who have complete visibility of the corporate risk register.

We have put together an overarching corporate security policy with an information risk management policy.

Engagement and Training

Users play an integral role in the defence against cybercrime. By acting as a 'human firewall', they often provide the last layer of defence between a 'rogue' agent attempting to gain unauthorised access to the organisation.

We run regular security awareness campaigns empowering staff to put security at the forefront of their projects and development.

Staff are encouraged to become more involved in reporting cyber security incidents, as this can lead to earlier detection of incidents that maybe missed by technology.

Senior members of the organisation are encouraged to lead by example and support our policies and procedures that underpin cyber security.

Asset Management

We maintain an inventory of assets to identify what technology and information assets are held within the organisation. This helps to:

- Identify what controls need to be put in place to protect the assets
- Identify hardware refresh requirements
- Facilitate the removal of legacy systems

All information assets are assigned an owner; they are then held accountable for the secure management of those assets.

All information assets are classified and a retention policy applied to ensure the organisation only keeps what is required to meet regulatory requirements and remain operational.

All assets that are identified to have associated vulnerabilities are prioritised for remedial action and entered into the risk register.

Architecture and Configuration

Getting security right at the start of any development helps to create systems that are easier to keep secure and can reduce the need for costly re-work in the future. We place cyber security on the agenda at the start of the design process accordingly to:

- Design, build, maintain and manage systems securely
- Make systems easy to maintain and update
- Make compromise and disruption difficult
- Reduce the impact of compromise
- Make it easy to detect and investigate compromises
- Safely develop and manage systems

Vulnerability Management

To protect against the exploitation of vulnerabilities, we implement a robust patch management regime:

- By reducing the number of vulnerabilities on the network we reduce the window of opportunity any malware has of exploiting an unpatched system.
- By hardening the systems before deployment, we reduce the number of services that could be manipulated to give unauthorised access to the network or services.
- To protect against malware attacks, we deploy endpoint protection to all organisation owned devices and systems.
- We implement regular vulnerability scanning to identify unpatched or hard to patch systems. We use penetration testing to simulate attackers' behaviour and validate the protection that is in place.
- We implement a secure email gateway to perform email content scanning to block or alert end users to suspect phishing links, with multifactor authentication to prevent the use of stolen credentials. We also filter web content to block malicious web sites.

All these measures are implemented together to deliver a 'defence in depth' approach to securing company infrastructure and information systems.

Identity and Access Management

We manage the user account life cycle through comprehensive workflow to ensure that only authorised access to information systems is granted to end users as and when required. Internal moves are treated as new starters to ensure they do not accrue unnecessary privileges.

We have developed appropriate identity and access management policies and processes – onboarding (joiners, movers and leavers), pre-employment checks, creating online accounts, single sign on helps with revocation – 3rd party access all have NDAs.

We implement multifactor-authentication for all user accounts with an appropriate password policy.

We implement a user tiered model for admin access. Privileged domain administrators use separate accounts for day-to-day operations. Their activities are closely monitored.

We implement security monitoring to detect potential malicious behaviour including:

- Impossible travel
- Multiple failed account log on attempts
- Checks for leaked or weak passwords when new passwords are created

Data Security

To protect against external hackers we deploy a centralised security system which can offer intrusion prevention and intrusion detection to prevent them from carrying out repeated attempts to gain unauthorised access.

We implement logical and physical network segregation to stop any hackers that have breached the network security from traversing the network and seeking out further vulnerabilities.

Data which is classified as sensitive or confidential is protected in transit, at rest and at the end of life.

We maintain up-to-date, isolated, offline backup copies of all important data and seek assurances from third party managed services that they also have robust ransomware protection in place.

Logging and Monitoring

We enable security audit logging on all key information systems and core infrastructure. Monitoring is centralised and alerts are set to warn of any suspicious behaviour.

We keep a central log to identify trends of advanced persistent threats and enable a quick response to block any further attempted access.

All monitoring and storage of log data is carried out in accordance with the latest regulations to protect the integrity and confidentiality of the information captured.

Incident Management

We have established an organisation-wide incident response capability where roles and responsibilities have been defined. Specific individuals have been appointed to handle ICT incidents.

We conduct a 'lessons learned' review by logging the actions taken during an incident and review the process performance post incident, to see what aspects worked well and what could be improved.

Supply Chain Attack

We carry out due diligence whenever onboarding new suppliers and maintain an approved supplier list which is regularly reviewed. Existing suppliers are assessed on their own cyber security maturity and are required to meet the criteria stipulated in the Supplier Control Policy.

Removable Media Controls

The use of removable media across the organisation is strictly controlled to stop the uploading of malware. Users are aware of the dangers of using removable media and are instructed to only use company issued devices which are adequately protected to hold sensitive, confidential, or personal data.

Home and Mobile Working

Brady has extended the same corporate protection against cybercrime that office-based staff benefit from. Access to company network resources are only made available over the secure SSL VPN connection. Staff are instructed to pay particular attention to their work environment whilst working away from the office.

Incident Response and Responsive

If a cyber attack is identified, we immediately deploy a response to minimise impact and ensure an efficient recovery. All staff are instructed to contact our InfraOps team directly. After initial triage the InfraOps team invoke a full incident response team response and the incident is escalated as per the Security Incident Response Plan.

BRADY