CHUBB®

Chubb Cyber Enterprise Risk Management

Standard Proposal Form

This document allows Chubb to gather the needed information to assess the risks related to your information systems. If your information systems security policies differ between your companies or subsidiaries, please complete separate proposal forms for each information system.

Company Information

Company name:	Website:

Company headquarters (Address, City, Country, Postcode):	Year established:	Number of employees:

Please provide contact details for the client's CISO or other staff member who is responsible for data and network security:

Name (first and surname):	Email:	Role:	Phone:

Note that Chubb may use these contact details to support our insureds with information on additional cyber security services, vulnerability alerts, and other helpful cyber insights.

Company Profile

1. **Turnover** – Please describe how much turnover you generate annually:

Turnover	Estimated current year	Projected following year
Global Turnover / Gross Revenue	£	£
Percentage of global turnover currently generated from USA & Canada		%
Percentage of global turnover currently generated from online sales		%

2. **Business Activities -** Please describe what your company does to generate the turnover listed above, including subsidiary activities:

3. Is your business a subsidiary, franchisee, or smaller entity of a larger organisation? □Yes □No
If yes, please detail

4. Do you provide ANY services to, or trade with individuals or organisations in sanctioned territories including but not limited to Iran, Syria, North Sudan, Crimea Region, North Korea, Venezuela, and Cuba, or any territory that is subject to certain US, EU, UN, and/or other national sanctions restrictions? □ Yes □ No

5. **Scope of Activities** - Do you have any company or subsidiary offices domiciled outside of your country of headquarters for which coverage is required? □ Yes □ No

a. If yes, please provide additional information on where these entities are located, and what percentage of revenue is generated by each entity. If you need more space, please include as an attachment to this proposal.
Note: This information is to ensure that each of your entities are eligible for coverage in the countries in which you operate.

Additional commentary on business operations:

Data Privacy

1. For approximately how many unique individuals and organisations could you be required to notify in the event of a breach of **Personally Identifiable Information** (PII)?

2. For approximately how many unique individuals and organisations do you hold:

a. payment card information or financial account information

b. health information records

3. Is any payment card information (PCI) processed in the course of your business? □ Yes □ No

a. If yes, what is the estimated number of PCI transaction that you process annually?

b. Please describe your (or your outsourcer's) level of **PCI DSS** compliance:

□ Level 1 □ Level 2 □ Not Compliant (please describe)

□ Level 3 □ Level 4

Data and Information Security

1. Please indicate whether you have the following cyber and data governance, resourcing, and planning practices in place:

a. formal privacy policy approved by legal and management □ Yes □ No
b. formal information security policy approved by legal and management □ Yes □ No
c. formal data classification policy □ Yes □ No
d. dedicated staff member(s) governing data and system security □ Yes □ No
e. formal cyber-specific incident response plan that is tested at least annually □ Yes □ No
f. formal privacy law and regulation compliance monitoring □ Yes □ No
g. cyber security baseline is set at the central/top level for all subsidiaries to comply with □ Yes □ No

Additional commentary

2. Have you identified all of the privacy and network security regulations and compliance standards applicable to the regions in which you operate? □ Yes □ No □ Partial

3. Have you assessed your compliance with these requirements in the last 12 months? □ Yes □ No □ Partial

4. Please provide additional commentary on any non-compliance with relevant **Privacy Laws and Regulations** in applicable jurisdictions, along with plans in place to remediate:

5. Do you and others on your behalf or at your direction collect, store or transmit biometric information, including but not limited to fingerprints, retina scans, or time clocks that rely on individual identifiers? □ Yes □ No

*If yes – please complete the "**Biometric Information**" supplemental questions at the end of this document.*

6. Please complete the following questions as it relates to **Personally Identifiable Information** (PII) storage, protection, or minimisation:

a. If **PII** is segmented, please indicate the total number of unique individuals that would exist in a single database or repository

b. Is access to your databases with **PII** limited to a need-to-know basis? □ Yes □ No

c. Please indicate what other controls protect or minimise your **PII**:

□ **Microsegmentation**
□ Data tokenisation
□ **Enterprise or Integrated Data Loss Prevention** (DLP)
□ Data anonymisation
□ **Encryption** at database level
□ Data pseudonymisation
□ **Encryption** in transit

Other:

7. Do you outsource the processing of **PII** to data processor(s)?	□ Yes	□ No	□ Partial
a. Do you maintain written contracts with such providers at all times?	□ Yes	□ No	□ Partial
b. Do these contracts address which party is responsible for responding to a **Data Breach**?	□ Yes	□ No	□ Partial
c. Do you waive rights of recourse against data processors in the event of a **Data Breach**?	□ Yes	□ No	□ Partial

Additional commentary on **PII** storage and collection:

Technical Controls and Processes

Network structure and access

1. Are critical systems and applications hosted centrally? □ Yes □ No □ Partial

2. Please detail how your network has been structured or segmented in order to minimise lateral movement of malware or users within your organisation, or to minimise the chance that multiple services are impacted by the same issue or vulnerability:

Does this utilise:

□ VLAN
□ Host-based firewalls
□ Other:
□ Air-gap
□ Least privilege access controls
□ Firewall configuration (access control list)
□ Software Defined Networking (SDN)

3. Please indicate if any of the following apply:

□ External penetration testing conducted at least annually
□ Internal system penetration testing conducted at least annually
□ **Web Application Firewalls** (WAF) are applied in front of most critically external facing applications

4. Do you allow mobile devices (including laptops, tablets, and smartphones) to access company or network applications and resources? □ Yes □ No

a. What percentage of mobile devices are **Managed Devices**, or you have enabled and enforced a **Mobile Device Management** product?

– company issued laptops, tablets, and smartphones % □ N/A

– Bring Your Own Device (BYOD) (including laptops, tablets, and smartphones) % □ N/A

5. Does any part of your corporate network maintain remote access capability? □ Yes □ No
If yes, please complete the below:

a. How is remote access to your corporate network secured? (select all that apply)

□ VPN (Virtual Private Network)
□ SSO (Single Sign-on) via **MFA**
□ Traffic **Encryption**
□ **Multi-Factor Authentication**
□ **ZTNA (Zero Trust Network Access)**
□ Other

b. Does the above apply to standard employees, contractors, vendors, suppliers, and privileged users that have remote access to your corporate network? □ Yes □ No □ Partial

Please detail any exceptions to the above, or provide additional commentary:

6. Please detail your use of **Remote Desktop Protocol** (RDP):

□ RDP is not used at all
□ RDP is limited to internal use only
□ RDP is used for remote access
□ RDP is used in another capacity:

a. If RDP is used in any capacity, which of the following are implemented? (select all that apply)

□ VPN (Virtual Private Network)
□ NLA (Network Level Authentication)
□ Other
□ **Multi-Factor Authentication**
□ RDP honeypots established

Directory, Domains, and Accounts

7. Do you have a formal **Identity and Access Management** programme in place? □ Yes □ No

8. Please detail your number of:

a. Service accounts

b. Users that have administrative access

c. Users that have persistent administrative access to workstations and servers other than their own

d. Privileged users that have full access to your directory service, including **Active Directory Domain**?

9. Please detail why this number of **Privileged Accounts** is necessary, and any planned actions to reduce this number:

10. Please indicate other controls are in place to manage accounts:

□ Local and domain accounts are regularly audited to check for unauthorised creation of new accounts
□ Access logs are stored for at least 90 days
□ Network administrators have separate "regular" and "privileged" accounts with separate authentication
□ **Privileged Access Workstations** are utilised
□ **Privileged Accounts** and directory services (including **Active Directory**) are monitored for unusual activity
□ **Privileged Accounts** are controlled by a **Privileged Access Management** (PAM) solution
□ Privileged access require separate **Multi-Factor Authentication** for internal or on-network access

Please detail any exceptions to the above, or provide additional commentary related to access controls, directory services (including **Active Directory Domain**), and **Privileged Accounts**:

Authentication

11. Where you have implemented **Multi-Factor Authentication**, has this solution been configured in a way where the compromise of any single device will only compromise a single authentication factor? □Yes □No □N/A
Additional commentary:

Email Security

12. Please detail how your email activity is secured (select all that apply):

□ **MFA** is required for webmail or cloud-hosted email
□ **Sender Policy Framework** (SPF) enforced
□ Secure email gateway enforced
□ All suspicious emails automatically quarantined
□ Sensitive external emails are sent securely
□ Microsoft Office macros are disabled by default
□ Applicable emails tagged as "External" or similar
□ **Domain Keys Identified Mail** (DKIM) is enforced
□ All incoming email is scanned and filtered for malware
□ **Sandboxing** is used for investigation of email attachments
□ Employees trained on phishing / social engineering threats
□ Other:

Additional commentary on email security:

Business Continuity and Disaster Recovery

13. Do you have a formal Business Continuity Plan that addresses cyber scenarios, tested annually? □Yes □No

14. Do you have a formal Disaster Recovery Plan that addresses cyber scenarios, tested annually? □Yes □No

15. Please provide some additional details on your ransomware-safe backup strategies related to disaster recovery:

□ Immutable or **Write Once Read Many** (WORM) backup technology utilised
□ Completely **Offline / Air-gapped** (tape / non-mounted disks) backups disconnected from the rest of your network
□ Restricted access via separate privileged account that is not connected to **Active Directory** or other domains
□ Restricted access to backups via **MFA**
□ **Encryption** of backups
□ Cloud-hosted backups segmented from your network
□ Other:

16. Please indicate if the following backup planning and testing practices are applicable:

□ Full restore from backup tests performed
□ Integrity of data is analysed when testing
□ Data scanned for malware prior to backup
□ Recoverability of data is tested
□ Restore plan includes specific ransomware scenarios
□ Backup procedures exist for email records

17. Please describe the information systems, applications, or services (both internally and externally hosted) on which you depend most to operate your business:
Regarding outsourced services, this may include cloud services, data hosting, business application services, co-location, data back-up, data storage, data processing, or any similar type of outsourced computing or information services.

Name of System, Application, or Service	Provider Name (if outsourced) *If internal put "N/A"*	Has a Business Impact Analysis been performed?

18. Do you maintain alternative systems for critical applications? □ Yes □ No □ Partial

19. Do you have alternate power for mission critical or revenue generating equipment? □ Yes □ No

20. Do you have the ability to procure extra bandwidth from alternative suppliers? □ Yes □ No

21. Do you use and test backup power generators, dual supply units, or other equipment to offset power outage or failure as part of business continuity or disaster recovery plans? □ Yes □ No

22. Do your software developers receive training on the principles of writing secure applications? □ Yes □ No

23. Please describe quality control and testing procedures that apply to any new software programmes (including updates and new releases to existing software) on your network (including minimal timeframe for a new or updated system to pass quality assurance testing before it is made operational on your live network, along with separate development, testing, and acceptance environments)

Prevention, Monitoring, and Incident Response

24. Do you have plans and protections in place for Distributed Denial of Service (DDoS) attacks? □ Yes □ No

25. How do you prevent, monitor and respond to cyber incidents and alerts (select all that apply)

- □ **Intrusion Detection System**
- □ Intrusion Prevention System
- □ **URL filtering or Web Filtering**
- □ **Application Isolation & Containment**
- □ **Security Orchestration, Automation, and Response** (SOAR) solution
- □ **Protective Domain Name System** (DNS) service
- □ **Threat Intelligence** sources or services used
- □ Advanced or next-generation anti-malware and anti-virus with **Heuristic Analysis**
- □ Manual Log reviews
- □ **Security Operations Centre** (SOC) in place
- □ Managed firewall service

Other monitoring tools or services (please detail):

□ **Advanced Endpoint Protection:**

- □ **Endpoint Detection and Response (EDR)**
- □ **Managed Detection and Response (MDR)**
- □ **Extended Detection and Response (XDR)**

Provider Name(s)

Percentage of endpoints covered by EDR, MDR, or XDR: %

Is this configured to automatically isolate or block activity? □ Yes □ No □ Partial

26. What percentage of alerts from EDR, MDR, or XDR feed into a **Security Information and Event Monitoring** (SIEM), **Security Orchestration, Automation, and Response** (SOAR), or **Centralised Endpoint Protection Platform** (or similar) system? % □ N/A

Asset and Configuration Management

27. Do you maintain an inventory of hardware and software assets? □ Yes □ No

a. What percentage of your assets is included in this inventory? %

b. What percentage of your assets are within scope for vulnerability scanning? %

28. How often do you perform vulnerability scans? Internal: External:

29. Do you assign risk levels for each asset in your inventory to prioritise patching and vulnerability management actions? □ Yes □ No

30. Do you operate any end-of-life or unsupported hardware, software, or systems? □ Yes □ No

If yes, please outline your use of end-of-life or unsupported hardware, software, or systems:

a. Are any of these processes, systems, or applications business-critical? □ Yes □ No

b. Do you store or process sensitive personal or corporate confidential information on these systems? □ Yes □ No

c. Are these systems restricted from internet access? □ Yes □ No □ Partial

d. Are these systems segregated and isolated from other parts of your network? □ Yes □ No □ Partial

e. Please outline which end-of-life or unsupported systems you operate, what they are used for, and how many are used in your business:

f. Please outline your decommissioning plans and timelines for these systems:

g. Please outline other mitigating controls in place to minimise lateral movement from unsupported systems to other environments within your network:

31. Do you regularly scan for and disable any unnecessary open ports and protocols? □ Yes □ No

32. Do you have a formal patch management process in place? □ Yes □ No

33. Please provide target timelines depending on vulnerability criticality (**Common Vulnerability Scoring System** – CVSS)

Low: days Medium: days High: days Critical: days

a. Please detail your level of compliance with these targets over the most recent 12 months:

34. If a patch can not be applied in a timely manner, what actions do you take to mitigate vulnerability risk?

Additional commentary on asset and patch management:

Third Party Risk Management

For this section, third parties technology providers may include cloud services, data hosting, business application services, co-location, data back-up, data storage, data processing, or any similar type of outsourced computing or information services.

1 . Do you perform risk-based assessments on which technology vendors are most critical to your business? □ Yes □ No □ Partial

2. Please select what is included in vendor assessments, either prior to contracting or during audits:

□ Information security certification review
□ Penetration testing
□ Cyber security rating service
□ **Multi-Factor Authentication** review
□ Data Protection Agreements included in contracts
□ Business resilience certification review
□ Review of vendor's backup procedures
□ Service Level Agreement (SLA) assessment
□ Data Protection Impact Assessment performed
□ Other:

3. How often do you waive your right of recourse against any third party technology providers in the event of service disruption?

□ Never or infrequently □ Sometimes □ Always or most of the time

Other commentary:

Cloud Security

4. Do you utilise cloud applications, platforms, infrastructure, or other services? □ Yes □ No

5. Do you have a formal cloud security policy? □ Yes □ No □ N/A

6. Please indicate which of the following you have implemented to support cloud security initiatives:

□ **Cloud Access Security Broker** (CASB)
□ **Zero Trust Network Access** (ZTNA) model enforced
□ **MFA** required for business critical cloud applications
□ Other:
□ **Secure Access Service Edge** (SASE) model enforced
□ Single Sign On (SSO) used for authentication
□ **MFA** required for non-business critical cloud applications

Media

1. Has legal counsel screened the use of all trademarks and service marks, including your use of domain names and metatags, to ensure they do not infringe on the intellectual property rights of others? □ Yes □ No
2. Do you obtain written permissions or releases from third party content providers and contributors, including freelancers, independent contractors, and other talent? □ Yes □ No
3. Do you involve legal counsel in reviewing content prior to publication or in evaluating whether the content should be removed following a complaint? □ Yes □ No
4. Do you contract with third parties providers, including outside advertising or marketing agencies, to create or manage content on your behalf? □ Yes □ No
   - **a.** If yes, do you require indemnification or hold harmless agreements in your favour? □ Yes □ No
5. Has your privacy policy, terms of use, terms of service and other customer policies been reviewed by counsel? □ Yes □ No

Loss History

1. Please indicate which of the following you have experienced in the past five years (please do not indicate events that have been mitigated by existing security measures):

   □ **Data Breach**
   □ **System Failure Event**
   □ Regulatory Actions related to data or system security
   □ **Cyber Incident** impacting a third party provider of yours
   □ Malicious **Cyber Incident** against you
   □ **Media Claim**
   □ **Data Breach** at a third party provider of yours

   a. If yes to any of the above, please provide:

   Description of any claims/incidents and date of occurrence:

   Description of the financial impact to your business:

   Mitigating steps you've taken to avoid similar future events:

2. Are you aware of any notices, facts, circumstances, or situations that could qualify as a **Data Breach**, **Cyber Incident**, **System Failure Event** or reasonably give rise to any **Media Claim** or Cyber or Data related Regulatory Actions? □ Yes □ No

   a. If yes, please provide additional details:

Supplemental Questions - only complete these sections if applicable to your business

Biometric Information

1. Do you collect biometric information from:
   - **a.** Employees □ Yes □ No
   - **b.** Service Providers or Contractors □ Yes □ No
   - **c.** Customers □ Yes □ No
   - **d.** Other (please specify): □ Yes □ No

2. Regarding biometrics collected, used, or stored on employees:
   - **a.** Do you receive written consent and a release from each individual? □ Yes □ No
   - **b.** Do you require each employee to sign an arbitration agreement with a class action waiver? □ Yes □ No

3. Do you have formal written policies pertaining to biometric information privacy requirements that clearly addresses retention and destruction guidelines? □ Yes □ No

4. Is written consent always obtained, and is this explicit consent? □ Yes □ No

5. When did you start collecting, storing, or processing biometric data?

6. How long have you had requirements for explicit written consent?

7. Please detail how many biometric information records you hold or are responsible for:

Operational Technology

For this section, operational technology (OT) differs from information technology (IT) in that OT is focused on monitoring, managing, and controlling industrial operations or physical equipment, while IT is focused on electronic data exchange, processing, and storage. Operational Technology may include Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), Distributed Control Systems (DCS), robotics systems, and more.

1. Do you have a formal OT security policy that includes cyber security? □ Yes □ No

2. Who is responsible for implementing and maintaining the cyber security of OT systems and networks?

□ IT security organisation
□ Engineering or business unit
□ Other:

3. How many production sites do you operate?

a. What percentage are:

operated by you %   operated by a provider %

4. Are production sites segmented from one another to minimise the chance of multiple sites being impacted by the same event or incident? □ Yes □ No

5. How do you segregate OT from Information Technology assets and networks?

□ VLAN
□ Air-gap
□ Demilitarised zoning (DMZ)
□ Other:

□ Data Diode
□ Host-based firewalls
□ Least privilege access controls

□ Firewall configuration (access control list)
□ OT has restricted Internet access

6. Do you allow remote access to OT environments? □ Yes □ No

If yes, please complete the below:

a. How is remote access to OT secured? (select all that apply)

□ VPN (Virtual Private Network)
□ SSO (Single Sign-on) via MFA
□ Traffic **Encryption**

□ **Multi-Factor Authentication**
□ **Zero Trust Network Access** (ZTNA)
□ Other:

Please detail any exceptions to the above, or provide additional commentary:

7. Please describe your patch management process and cadence for OT

8. Do you monitor and respond to events occurring in your OT environment in the same way as your Information Technology environment? □ Yes □ No

9. Do you maintain and test backups of your OT environment? □ Yes □ No

a. If yes, how are these backups protected? (select all that apply):

□ Immutable or **Write Once Read Many** (WORM) backup technology
□ Completely **Offline / Air-gapped** (tape / non-mounted disks) backups
□ Restricted access via separate privileged account that is not connected to **Active Directory** or other domains
□ Restricted access to backups via **MFA**
□ **Encryption** of backups
□ OT backups are segmented from IT networks
□ None of the above
□ Other:

10. Please describe your ability to rely on manual or other workaround procedures if systems are impacted by cyber incident:

Acquisitions

1. How many acquisitions have you made over the past three years?

2. Please detail name of entities acquired, size of entities, and dates of acquisitions:

3. When do you audit and assess the cyber security posture and exposure of such entities?

□ Before acquisition
□ After acquisition but before integration
□ Assessments of cyber security are rarely performed before or after acquisition
□ Other:

4. Please detail integration strategy, timelines, and due diligence performed regarding acquired entities:

Professional Services

1. Do you purchase any professional indemnity insurance? □ Yes □ No

2. If yes, does your policy contains any applicable cyber exclusions? □ Yes □ No

3. Do you operate, manage, or host any technology systems in support of your professional services? □ Yes □ No

a. Are data and systems related to such services the responsibility of your customer? □ Yes □ No
Please detail:

b . If you do host data and systems for your customers, do controls described in this proposal form apply to these hosted systems as it relates to resiliency, backup strategies, and data privacy compliance? □ Yes □ No

Additional commentary:

Retail Operations

1. Do you segregate your Point of Sale or transaction processing equipment and networks from other IT networks? □ Yes □ No

2. Please describe your patch management process and cadence for Point of Sale software applications:

3. What percentage of Point of Sale / payment terminals that support chip technology meet EMV standards? %

4. Please name the provider(s) you rely on for payment processing:

5. Are Point of Sale systems protected by antimalware and monitored by your information security resources? □ Yes □ No
Additional commentary:

6. Do you have any franchisee locations or agreements? □ Yes □ No

a. If yes, please provide more information on who is responsible for cyber security at franchisees, and how cyber security controls are consistently applied:

Cyber Improvements (Optional)

Please outline what improvements you have planned for the next ~12 months as it relates to cyber or information security and management:

Coverage

1. Please provide details of your current insurance policies (if applicable).

Coverage – tick if current policy in place	Limit	Excess	Premium	Insurer	Expiry Date (DD/MM/YYYY)
Cyber	£	£	£		/ /
Crime	£	£	£		/ /
Professional Indemnity	£	£	£		/ /

2. Please indicate the limits for which you would like to receive a quote.

Coverage	Limit				
Cyber Expenses	□ £1m	□ £2m	□ £3m	□ £5m	□ Other £
Cyber Liability	□ £1m	□ £2m	□ £3m	□ £5m	□ Other £

Declarations

I declare (i) that we have made a fair presentation of the risk, by disclosing all material matters which we know or ought to know or, failing that, by giving the Insurer sufficient information to put a prudent insurer on notice that it needs to make further enquiries in order to reveal material circumstances; and that (ii) I have obtained, and will obtain in the future, the express consent to the disclosure and use of sensitive personal data from every data subject whose sensitive personal data is supplied in relation to this proposal for the purposes of (a) underwriting the risks and (b) administering and performing any resulting insurance contract. I undertake to inform the insurer promptly in writing of any material alteration to those facts occurring before completion of the contract of insurance.

Name of Director, Officer, or Risk Manager:

Signature of Director, Officer, or Risk Manager:

Date (MM/DD/YYYY):

/ /

Optional Services Questionnaire

Chubb has partnered with a number of cyber security vendors that can help you manage your cyber risk. In order to provide you with meaningful services, you may answer the few questions below. More information on our Loss Mitigation Services can be found at **www.chubb.com/cyber-services**

1. Do you engage your employees in phishing training exercises on a regular basis? □ Yes □ No
2. Do you use enterprise password management software to encourage responsible password practices? □ Yes □ No
3. Do you provide your employees with any cyber-related training modules to encourage cyber best practices? □ Yes □ No
4. Have you engaged in any planning, testing, or training in regards to cyber incident response preparedness? □ Yes □ No

Glossary of Terms

Active Directory Domain – is a collection of objects within a Microsoft Active Directory network. An object can be a single user or a group, or it can be a hardware component, such as a computer or printer. Each domain holds a database containing object identity information.

Advanced Endpoint Protection – is a device or software that provides protects and monitors the endpoints on your network. Endpoints include desktop and laptop computers, tablets, mobile phones, servers, and any other device connected to your network.

Application Isolation & Containment – this technology can block, restrict, or isolate specific endpoints from performing potentially harmful actions between endpoints and other applications or resources with the goal to limit the impact of a compromised system or endpoint.

Centralised Endpoint Protection Platform – is a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

Cloud Access Security Broker (CASB) – is software that monitors the activity between cloud service users and cloud applications to enforce security policies and prevent malicious activity.

Common Vulnerability Scoring System (CVSS) – is an open industry standard assessment of the severity of vulnerabilities, assigning scores depending on ease and potential impact of exploits.

Configuration Management Databases (CMDB) – is a database used to store information on hardware and software assets of an organisation, and is typically used to identify and manage the configuration of and the relationship between assets.

Cyber Incident – includes unauthorised access to your computer systems, hacking, malware, virus, cyber extortion, distributed denial of service attack, insider misuse, human or programming error, or any other cyber-related event.

Data Breach – means an incident where sensitive personal or corporate confidential information has been taken, lost, or viewed by an unauthorised party.

Domain Keys Identified Mail (DKIM) – is a standard email authentication method that adds a digital signature to outgoing messages to allow for improved verification of sender.

Encryption – is the method of converting data from a readable format to an encoded format. It can only become readable again with the associated decryption key.

Endpoint Detection and Response (EDR) – is a solution which records and stores endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems.

Enterprise or Integrated Data Loss Prevention (DLP) – are software products and rules focused on preventing loss, unauthorised access, or misuse of sensitive or critical information. Enterprise DLP describes dedicated solutions implemented across an organisation and may include alerts, encryption, monitoring, and other movement control and prevention for data at rest and in motion. Integrated DLP utilises existing security tool services and add-ons to accomplish the same goal of preventing data loss and misuse.

Extended Detection and Response (XDR) – is a security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components, typically including endpoints, networks, servers, cloud services, SIEM, and more.

Heuristic Analysis – going beyond traditional signature-based detection in basic antivirus software, heuristic analysis looks for suspicious properties in code, and can determine the susceptibility of a system towards particular threat using various decision rules or weighing methods designed to detect previously unknown computer viruses, as well as new variants of viruses already in the "wild".

Identity and Access Management (IAM) – ensures that the right users have the appropriate access to technology resources, and includes the management of usernames, passwords, and access privileges to systems and information

Intrusion Detection Systems (IDS) – is a device or software that monitors your network for malicious activity or policy violations.

Managed Detection and Response (MDR) – is a managed cyber security service that provides intrusion detection of malware and malicious activity in your network, and assists in rapid incident response to eliminate those threats with succinct remediation actions.

Managed Device – is a device that requires a managing agent or software tool that allows information technology teams to control, monitor, and secure such device. A non-managed device would be any device that can not be seen or managed by such products or technology teams.

Media Claim – includes any claim for product disparagement, slander, trade libel, false light, plagiarism, or similar from your website or social media accounts.

Microsegmentation – is a network security technique that enables security architects to logically divide the data center into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment.

Mobile Device Management (MDM) – is software that is installed on a managed device that allows information technology administrators to control, monitor, and secure mobile device endpoints.

Multi-Factor Authentication (MFA) – MFA is an electronic authentication method used to ensure only authorised individuals have access to specific systems or data. A user is required to present two or more factors – these factors being 1) something you know, 2) something you have, or 3) something you are. Something you know may include your password or a pin code. Something you have may include a physical device such as a laptop, mobile device that generates a unique code or receives a voice call or a text message, a security token (USB stick or hardware token), or a unique certificate or token on another device. Something you are may include biometric identifiers.

Note that the following are not considered secure second factors: a shared secret key, an IP or MAC address, a VPN, a monthly reauthentication procedure, or VOIP authentication.

Offline or Air-gapped – as it relates to backup solutions, offline or air-gapped storage means that a copy of your data and configurations are stored in a disconnected environment that is separate to the rest of your network. Physical tape or non-mounted disk backups that aren't connected to the internet or LAN would be considered offline.

PCI DSS – PCI DSS stands for the Payment Card Industry Data Security Standard. This defines the requirements that a company must comply with if they handle any payment card information.

Personally Identifiable Information (PII) – means any data that can be used to identify a specific individual. This may include health or medical records of employees or customers, government issued identification numbers, login usernames, email addresses, credit card numbers, biometric information, and other related personal information.

Privacy Laws and Regulations – describes the body of law that sets the requirements and regulations for the collection, storage, and usage of personally identifiable information, personal healthcare information, financial information of individuals, and other sensitive data which may be collected by public or private organisations, or other individuals.

Privileged Access Management (PAM) – describes enterprise processes and technology supporting Privileged Accounts. PAM solutions offer an additional layer of protection, and typically have automated password management, policy enforcement capabilities, account lifecycle management capabilities, as well as monitoring and reporting of privileged account activity.

Privileged Access Workstations – is a hardened workstation configured with security controls and policies that restrict local administrative access and productivity tools to minimise the attack surface to only what is absolutely required for performing sensitive job tasks. These workstations typically have no access to email or general web browsing.

Privileged Accounts – means accounts that provide administrative or specialised levels of access based on a higher level of permission.

Protective Domain Name System – is a service which prevents access to domains known to be malicious, and also allows for additional analysis and alerts regarding blocked domain requests.

Remote Desktop Protocol (RDP) – is a Microsoft protocol that allows for remote use of a desktop computer. Without additional protections, RDP has some serous security vulnerabilities.

Sandboxing – as it relates to email solutions, a sandbox filters emails with unknown URL links, attachments, or other files, allowing them to be tested in a separate and safe environment before allowing them to proceed to your network or mail servers.

Secure Access Service Edge (SASE) – is a cloud-delivered service that combines cloud based network and security functions such as SWG, CASB, ZTNA with WAN capabilities.

Security Information and Event Monitoring (SIEM) – is technology and related services that provide real-time analysis of cyber security alerts from a collection of sources, including endpoints and applications to allow for improved detection, compliance enforcement, and incident management.

Security Operations Centre (SOC) – is a centralised function involving people, processes, and technology designed to continuously monitor, detect, prevent, analyse, and respond to cyber security incidents.

Security Orchestration, Automation, and Response (SOAR) – is technology used to automatically streamline and prioritise cyber security alerts from a collection of sources, including endpoints and applications (similar to a Security Information and Event Monitoring solution) but offers enhanced automated response and improved prediction techniques.

Sender Policy Framework (SPF) – is an email authentication method that is used to prevent unauthorised individuals from sending email messages from your domain, and generally helps to protect email users and recipients from spam and other potentially dangerous emails.

Single Sign On (SSO) – is a method of authentication that enables users to authenticate securely with multiple applications and websites without logging into each one individually. This involves a trust relationship set up between an application, known as the service provider, and an identity provider.

System Failure Event – is the unintended breakdown, outage, disruption, inaccessibility to, or malfunction of computer systems or software caused by non-malicious means. A system failure event may be caused by a power failure, human error, or other disruption.

Threat Intelligence – is information on current security threats, vulnerabilities, targets, bad-actors, and implications that can be used to inform security decisions.

URL Filtering or Web Filtering – is technology that restricts which websites a user or browser can visit on their computer, typically filtering out known malicious or vulnerable websites.

Web Application Firewall (WAF) – is a type of network, host, or cloud-based firewall placed between an application and the Internet to protect against malicious traffic, and other common web attacks that typically target sensitive application data.

Write Once Read Many (WORM) – is a data storage device in which information, once written, cannot be modified.

Zero Trust Network Access (ZTNA) – is a service involving the creation of an identity and context-based, logical access boundary around an application or set of applications.

Contact us

Chubb European Group SE
The Chubb Building, 100 Leadenhall Street
London, EC3A 3BP

T: 020 7173 7000
F: 020 7173 7800
www.chubb.com/uk

Data Protection Notice

We use personal information which you supply to us or, where applicable, to your insurance broker for underwriting, policy administration, claims management and other insurance purposes, as further described in our Master Privacy Policy, available here: https://www2.chubb.com/uk-en/footer/privacy-policy.aspx. You can ask us for a paper copy of the Privacy Policy at any time, by contacting us at dataprotectionoffice.europe@chubb.com.