exponential-e
APPLIED INNOVATION

DATA SHEET
CYBER SECURITY SERVICES

Cyber Security Diagnostics Assessment

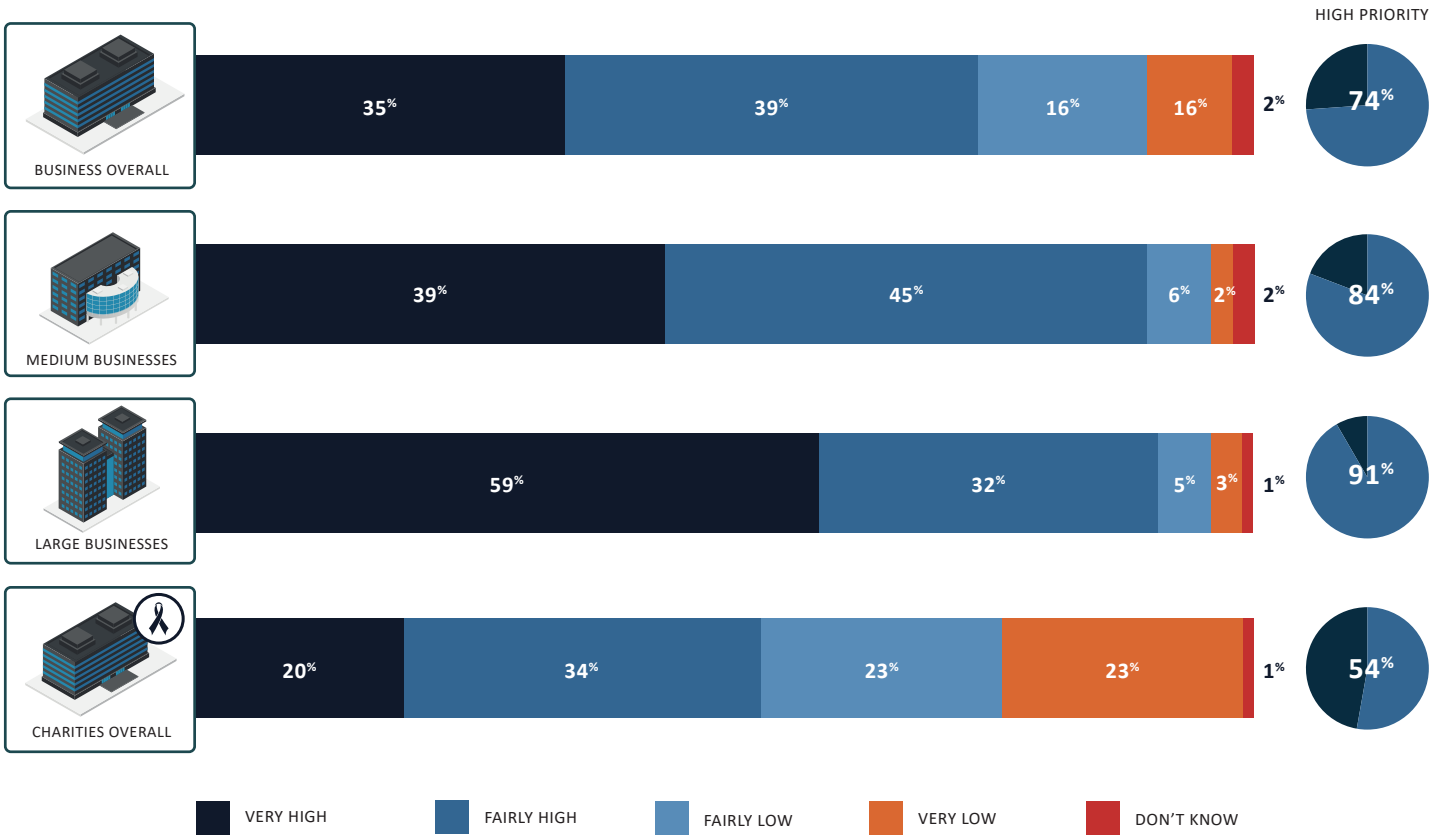
How cyber-secure is your business?

In 2018, it was reported in the Department for Digital, Culture, Media and Sport's 'Cyber Security Breaches Survey 2018' that (43%) and two in ten charities (19%) in the UK had experienced a cyber security breach or attack in the last 12 months. International standards such as the EU GDPR and requirements such as corporate governance and supply chain management now make demonstrable cyber security risk management a critical consideration for modern businesses.

Staying informed about your cyber security posture is crucial, but it can easily become overcomplicated and expensive. That's why Exponential-e has produced the Cyber Security Diagnostic Assessment (CSDA).

The Department for Digital, Culture, Media and Sport's 'Cyber Security Breaches Survey 2018' further reported that 72% of large organisations and 64% of small and medium-sized businesses (SMEs) had experienced a security breach of some sort. Major breaches cost large organisations, on average, between £1.46 and £3.14 million, and cost SMEs between £75,000 and £310,800.

Q. How high or low a priority is cyber security to your organisation's directors, trustees or senior management?



Exponential-e Ltd
100 Leman Street, London
E1 8EU

Telephone
+44 (0) 845 470 4001

Visit the website
www.exponential-e.com

Email
info@exponential-e.com

Follow us on Twitter
@exponential_e

Cyber Security Diagnostics Assessment (CSDA)

Compliance assessment to ISO 27001

What is the CSDA?

The CSDA quickly, efficiently and at low cost enables organisations of all sizes to assess their cyber security position, inform their decision-making and increase resilience.

The CSDA provides your business with one-on-one time with Exponential-e's experienced and qualified cyber security consultants. Working with you, our team will explore and evaluate your cyber security position in order to:

- Improve your understanding of current threats to you and your industry
- Provide actionable advice as to the required steps to improve your business's cyber resilience
- Assess your company's cyber profile against best practices and industry certifications (such as Cyber Essentials and ISO 27001)

Our consultants will deliver a personalised CSDA report that will:

- Clearly communicate your cyber security position
- Assess whether best practices are being followed
- Target and prioritise existing cyber security risks
- Provide practical advice to mitigate risks and remediate issues
- Provide a baseline summary to enable strategic planning of cyber security policies
- Assist with compliance to national and international industry standards

Our consultants will talk through the CSDA report with your employees to ensure all findings are understood.

What's next?

Should you choose to implement some or all of our recommendations, Exponential-e can advise you on how to do so in a cost-effective manner. We can also provide ongoing cyber security support to your business, including in the following areas:

- Cyber policy advice
- Virtual cyber teams
- Cyber training for your employees
- Vulnerability testing, including phishing campaigns and penetration testing

You may of course wish to undertake any required work in-house, or use our findings to guide a third-party provider as to your requirements.

Exponential-e Ltd
100 Leman Street, London
E1 8EU

Telephone
+44 (0) 845 470 4001

Visit the website
www.exponential-e.com

Email
info@exponential-e.com

Follow us on Twitter
@exponential_e

What's next?

Section	Operational Security	Status	Notes
A12	**Operational Procedures and Responsibilities**		
A12.1	Documented operating procedures	Managed	Procedures for operational security (Firewall management in place and aligned to CIS Top20) Procedures updated annually and reviewed by a technical supplier that provides the technology - as a second option
A12.1.2	Change management	Defined	Change management process is new. Has the backing from management but is in its infancy.
A12.1.3	Capacity management	Initial	Limited capacity mangement in place. The systems are configured to generate the necessary logs for assessing and monitoring capacity management but currently are not sent to the SIEM (See 12.4.1)
A12.1.4	Separation of development, testing and operational environments	Defined	
A12.2	**Protection from malware**		
A12.2.1	Controls against malware		Robust approach and process in place. Sugnatures monitoring and updated. Secondary control (Vulnerability) help identify systems that are non-compliant for AV software
A12.3	**Backup**		
A12.3.1	Information		Cloud and AWS backups conducted every 6 hours. All back up data assessed for Ransomware following recent attack - which also affected the backup data
A12.3	**Logging and monitoring**		
A12.4.1	Event logging		Opportunity to consider a Managed Service. Skills required not-in-house. Network supplier have the ideal offering fo rthis organisation to implement.
A12.4.2	Protect of log information	Initial	Log data ad-hoc encryption. Manual and not automated.
A12.4.3	Administrator and operator logs	Initial	As above
A12.4.4	Clock synchronisation	Initial	Only key systems have UTM synchronisation. Risk here is the limited correlation of events to support forensic investigations if required.
A12.5	**Control of operational software**		