SOLUTIONS

COMPLETE SECURITY
It’s not a case of if, but when. And in some cases you’ve already been breached, you just didn’t know it.

The traditional approach to cyber security is broken. Spending has increased but so has the number of breaches and the sophistication of new threats.

Trends show a huge rise in phishing attacks and data breaches via increasingly common workplace sources such as mobile and IoT devices. According to research by Ipsos Mori Social Research Institute, around a third of businesses report having been the victim of cyber security breaches or attacks in the last 12 months.

Understanding your current risk profile and implementing the correct set of solutions and measures ensures your organisation can protect themselves from the smaller-scale mundane attacks to the more serious security attacks that have the potential to cause serious disruptions, brand or financial loss and even take an organisation down.

Security measures that are effective today may no longer provide the necessary protections tomorrow. The threat landscape is growing in size and complexity, and at an unprecedented pace.

- Growth of well-publicised major breaches suggests that not only are the number of security breaches going up, they’re also increasing in severity.
- Average cost of cybercrime is increasing dramatically, which can be crippling to companies that have not made cyber security a priority within their boardroom.
- With new threats emerging every day, the risks associated with inadequate measures to protect your key assets and data are higher and more dangerous than ever for business.

Security breaches increased by 67% in 5 years

Security measures that are effective today may no longer provide the necessary protections tomorrow. The threat landscape is growing in size and complexity, and at an unprecedented pace.

- Growth of well-publicised major breaches suggests that not only are the number of security breaches going up, they’re also increasing in severity.
- Average cost of cybercrime is increasing dramatically, which can be crippling to companies that have not made cyber security a priority within their boardroom.
- With new threats emerging every day, the risks associated with inadequate measures to protect your key assets and data are higher and more dangerous than ever for business.

Ransomware damage estimated to reach $20bn globally

To protect business continuity, it is crucial to assess your business’s security risk, implement the right solutions, ensure company-wide changes and improve overall security culture.
CDW’s structured approach minimises the likelihood of a security incident. We help organisations identify risk, protect against known threats, detect suspicious activity, provide incident response services and help organisations recover from a breach or security incident.

**FIVE KEY AREAS TO ADDRESS**

**DATA**
Structured, unstructured, some classified, some not, data sits everywhere and is expanding. Poor visibility of who or what is accessing the data or an insufficient access policy creates high risk. **Average company has 534,465 sensitive files.**

**USERS**
Do you know your user base? There are many different user types, and not just within your own organisation. Third parties, customers and potential cyber attackers all want to access your data. **85% of companies are struggling to achieve even basic Privileged Access Management (PAM) capabilities.**

**DEVICES**
With so many different users accessing your data, not only from workplace devices but from personal devices too, visibility and control can be more challenging, not to mention IoT and OT devices. **Of the 28 billion connected devices in use by 2020, 20 billion will be IoT devices that are prone to security attacks.**

**APPLICATIONS**
Your organisation will be using a range of applications, either to access or set up data. These will be delivered via a mix of on-premise and cloud-based solutions, all of which bring their own security risks and challenges. **46% of websites have high cyber security vulnerabilities.**

**INFRASTRUCTURE**
Understanding what threats and security risks lie within your infrastructure is paramount to providing resilient services to your organisation and clients on a 24/7 basis. **By 2024, workloads in the cloud will suffer 60% fewer security incidents than those in traditional data centres.**

**FIVE STEPS OF SECURITY SPANNING YOUR ORGANISATION**

**IDENTIFY**
It’s essential for every enterprise to have a clear understanding of the cyber security risk profile associated with them. Identifying risk is key within this approach and organisations must have a deeper understanding of where their data and applications reside, which has access to them, using what types of devices and where all of these are positioned within your infrastructure.

**PROTECT**
In order to address any issues that have been identified, cyber security solutions must increase integrity and security without impeding data availability. CDW orchestrates solutions based on your technical, security and business requirements, whilst factoring in identified risks. Our in-depth knowledge of the cyber security market, wealth of expertise and large portfolio of vendor partnerships enables us to design and deliver end-to-end solutions to address business challenges and reduce risk.

**DETECT**
What’s secure today isn’t necessarily secure tomorrow. The IT environment is ever-changing — from the adoption of new cloud services to deployment of new devices, applications or infrastructure refreshes — and every change presents its own individual risk. Whilst it’s important to protect what you have, it’s important to adapt new technology and services that provide clear visibility of new threats being introduced into your environment to provide a deeper insight into an organisation’s cyber security posture.

**RESPOND / RECOVER**
CDW’s structured approach minimises the likelihood of a security incident. However, an Incident Response Plan must be factored into your security strategy. This makes a fast and efficient response to a suspected breach or security incident, minimising damage and accelerating the resumption of normal operations. CDW can help formulate an Incident Response Plan and advise on the best solutions to help you restore data, service availability and business continuity.
CDW's Security Practice is led by knowledgeable and skilled consultants who have more than 20 years of cyber security experience, providing end-to-end solutions to help organisations combat the ongoing evolution of cyber threats, reduce risk and improve security maturity.

Our Practice is not aligned to any specific vendor or technology and takes an impartial approach to providing the best cyber security solutions to meet customers' business, technical and security requirements.

We offer to conduct high-level security reviews and assessments to help organisations understand more about their current security posture and identify priority areas to address.

Our Partnerships
An extensive array of partnerships with both large and specialist technology suppliers enables CDW to design best-in-class solutions with cyber security embedded at every level. This helps organisations avoid the vulnerabilities and costs of managing a piecemeal approach to cyber security. Instead of dealing with multiple vendors, enterprise organisations can have confidence in their partnership with a single solution provider dedicated to optimising resilience.

Our Capabilities

Security Practice
- Advisory
- Requirement gathering
- High Level Solution Design
- Proposals
- Demonstrations
- Proof of Concept
- High Level Security reviews

Professional Services
- Low Level Design
- Migration Planning
- Interoperability Validation
- Pre-Staging
- Onsite Deployment & Engineering
- Policy Testing
- Project & Programme Management
- Training / Education

Managed Services
- 24x7 Service Desk
- Support, Monitoring and Full Life-Cycle Management
- Services for Palo Alto, Check Point, Fortinet, Cisco and F5
- ServiceWorks Cloud Platform for Security
Over the past 5 years, security breaches have increased by 67%, according to Accenture’s global survey. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Cyber security Ventures predicts that a business will fall victim to a ransomware attack this year in its 2019 Official Annual Cybercrime Report (ACR). The company also estimates that number will increase to every 11 seconds by 2021.

The Cyber security Ventures annual crime report indicates that the same costs will reach $5.15B annually this year and $20B per year by 2021. Unsurprisingly, this type of year-over-year increase in anticipated damages makes ransomware the fastest-growing type of cybercrime in the last year. https://www Hemisphere.com/blog/80-eye-opening-cyber-security-statistics-for-2019/

Varonis 2019 Global Data Risk report – Page 4

Thycotic State of PAM Maturity Report

ForeScout

Acunetix Web Application Vulnerability Report 2019

https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/