Kris Daniels - Managing Director, Solve-IT

Summary - What is GDPR?

GDPR (General Data Protection Regulation) is the new European legal framework for the protection of personal data.

It has stronger rules on data protection and designed to give control back to citizens and residents over their personal data.

One set of rules for all companies operating in the EU, wherever they are based.

Personal Data

Special Category Data

What is Personal Data?

…any information relating to a natural person who can be directly or indirectly identified, in particular by reference to an identifier.

…applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

GDPR – An IT Guide To Protecting Your Data

My 5 Steps (+2) to Securing your Data (Cybersecurity)

1 Boundary controls

Protect the online doors and windows of the business. Firewalls prevent unauthorised access from the Internet and are an important control. Password protect wireless (WiFi) and avoid using public wireless for confidential business actions.

2 Access Control

Restrict access to valuable data and systems. Make sure accounts are cancelled when employees leave the company. Log out from computers when stepping away and monitor accounts with special permissions such as administrator accounts.

3 Secure Configuration

Using applications as they come 'out of the box' can be unsafe. Secure configuration is about limiting the opportunities for the attackers. Disable unused accounts and services. Use strong passwords and back up your data regularly.

4 Anti Malware

Anti-malware scan computers looking for malicious files and program behaviour. Make sure anti-malware is installed and set automatically check for updates to protect against your threats.

5 Patching

Stay safe by keeping systems up-to-date. Hackers target old and vulnerable systems. Patching can ensure automatic updates are enabled, including web browsers. Delete all programs that are not required for work.

6 Education

Fact.. Hackers will target users as they are typically the weakest part of the system.

Solution.. Provide regular training and briefings to staff on how to protect themselves online.

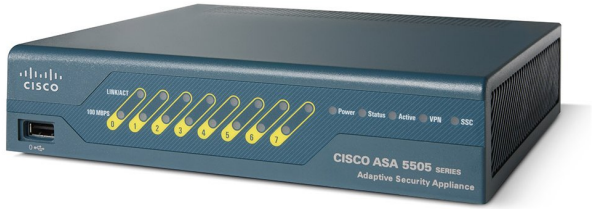
"Don't learn the hard way!!"

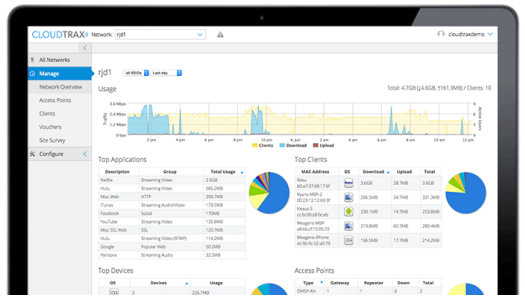
7 Incident Planning

Fact.. Hackers will rely on the fact that their targets will have not planned for the attack.

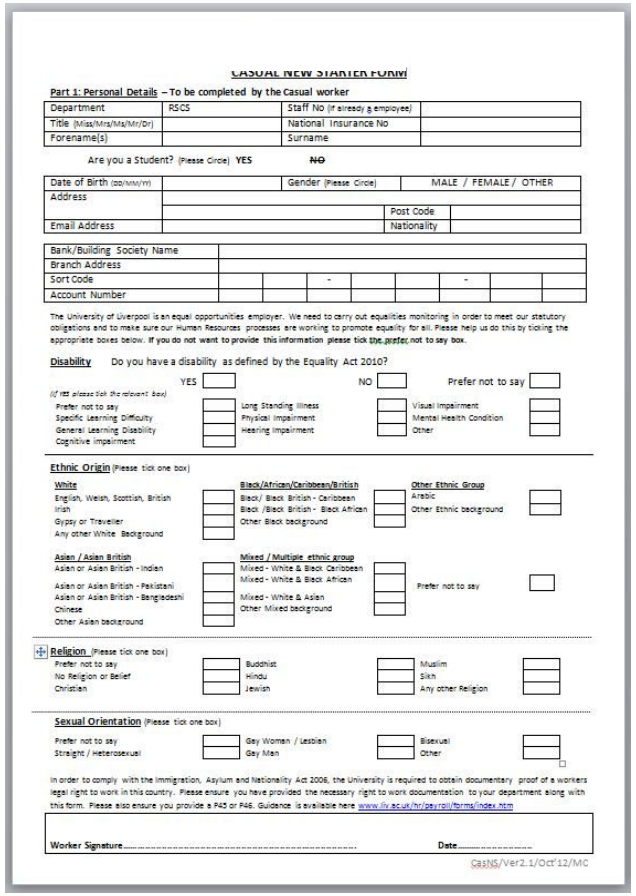
Solution.. Reduce the impact of the attack by having a plan in place to activate.

"Back in Business.. How long?"





My Recommended Boundary Controls



CASUAL NEW STARTER FORM

Part 1: Personal Details – To be completed by the Casual worker

Department	RSCS	Staff No (if already a employee)	
Title (Miss/Mrs/Ms/Mr/Dr)		National Insurance No	
Forename(s)		Surname	

Are you a Student? (Please Circle) YES ~~NO~~

Date of Birth (DD/MM/YY)		Gender (Please Circle)	MALE / FEMALE / OTHER
Address			
		Post Code	
Email Address		Nationality	

Bank/Building Society Name								
Branch Address								
Sort Code			-			-		
Account Number								

The University of Liverpool is an equal opportunities employer. We need to carry out equalities monitoring in order to meet our statutory obligations and to make sure our Human Resources processes are working to promote equality for all. Please help us do this by ticking the appropriate boxes below. If you do not want to provide this information please tick the prefer not to say box.

Disability Do you have a disability as defined by the Equality Act 2010?

YES ☐ NO ☐ Prefer not to say ☐

(If yes please tick the relevant box)

Prefer not to say ☐ Specific Learning Difficulty ☐ General Learning Disability ☐ Cognitive Impairment ☐ Long Standing Illness ☐ Physical Impairment ☐ Hearing Impairment ☐ Visual Impairment ☐ Mental Health Condition ☐ Other ☐

Ethnic Origin (Please tick one box)

White: English, Welsh, Scottish, British ☐ Irish ☐ Gypsy or Traveller ☐ Any other White Background ☐

Black/African/Caribbean/British: Black/ Black British - Caribbean ☐ Black /Black British - Black African ☐ Other Black background ☐

Other Ethnic Group: Arabic ☐ Other Ethnic background ☐

Asian / Asian British: Asian or Asian British - Indian ☐ Asian or Asian British - Pakistani ☐ Asian or Asian British - Bangladeshi ☐ Chinese ☐ Other Asian background ☐

Mixed / Multiple ethnic group: Mixed - White & Black Caribbean ☐ Mixed - White & Black African ☐ Mixed - White & Asian ☐ Other Mixed background ☐

Prefer not to say ☐

Religion (Please tick one box)

Prefer not to say ☐ No Religion or Belief ☐ Christian ☐ Buddhist ☐ Hindu ☐ Jewish ☐ Muslim ☐ Sikh ☐ Any other Religion ☐

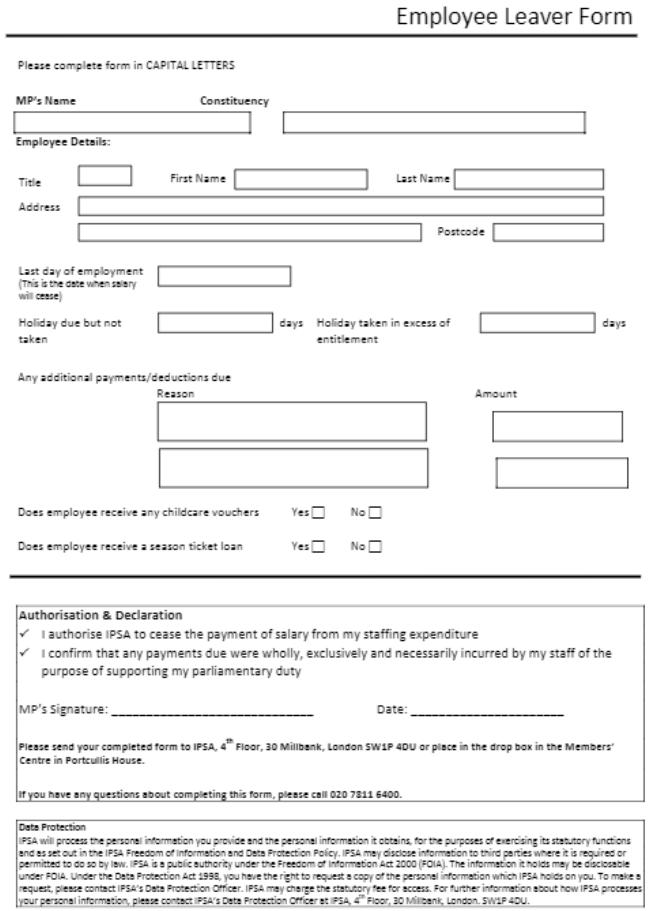
Sexual Orientation (Please tick one box)

Prefer not to say ☐ Straight / Heterosexual ☐ Gay Woman / Lesbian ☐ Gay Man ☐ Bisexual ☐ Other ☐

In order to comply with the Immigration, Asylum and Nationality Act 2006, the University is required to obtain documentary proof of a workers legal right to work in this country. Please ensure you have provided the necessary right to work documentation to your department along with this form. Please also ensure you provide a P45 or P46. Guidance is available here www.liv.ac.uk/hr/payroll/forms/index.htm

Worker Signature..... Date.....

CasNS/Ver2.1/Oct'12/MC



Employee Leaver Form

Please complete form in CAPITAL LETTERS

MP's Name ☐ Constituency ☐

Employee Details:

Title ☐ First Name ☐ Last Name ☐

Address ☐

☐ Postcode ☐

Last day of employment (This is the date when salary will cease) ☐

Holiday due but not taken ☐ days Holiday taken in excess of entitlement ☐ days

Any additional payments/deductions due

Reason	Amount

Does employee receive any childcare vouchers Yes ☐ No ☐

Does employee receive a season ticket loan Yes ☐ No ☐

Authorisation & Declaration

- ✓ I authorise IPSA to cease the payment of salary from my staffing expenditure
- ✓ I confirm that any payments due were wholly, exclusively and necessarily incurred by my staff of the purpose of supporting my parliamentary duty

MP's Signature: _____ Date: _____

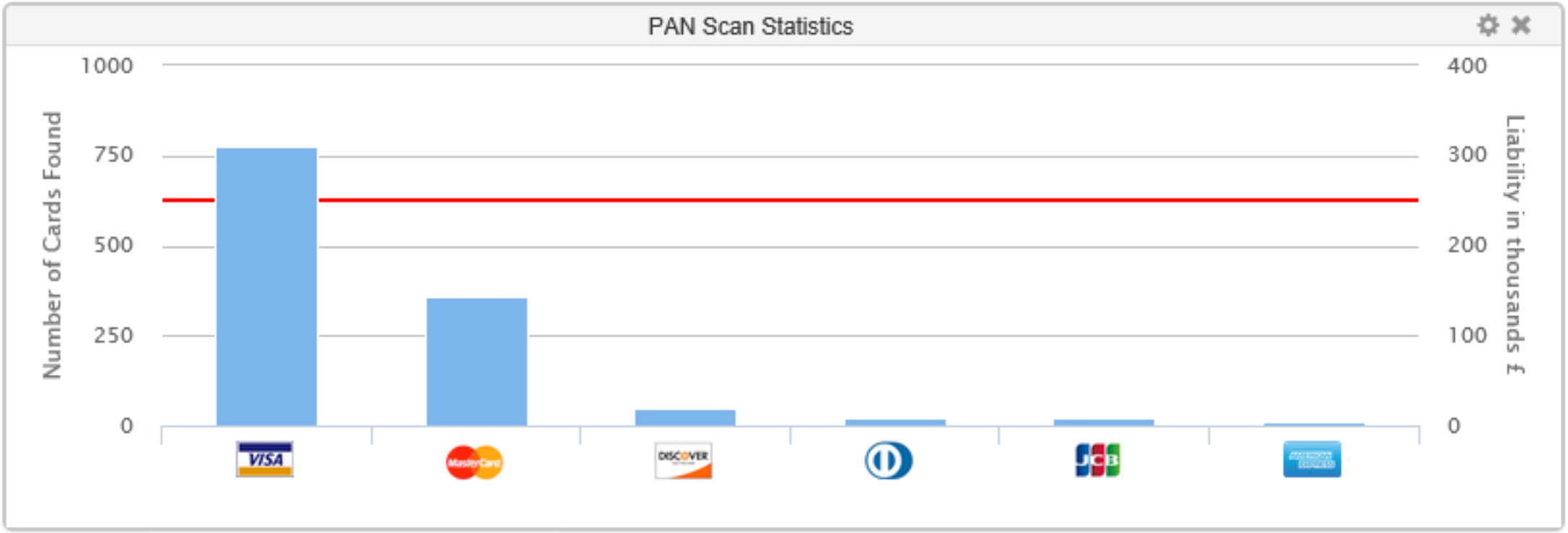
Please send your completed form to IPSA, 4th Floor, 30 Millbank, London SW1P 4DU or place in the drop box in the Members' Centre in Portcullis House.

If you have any questions about completing this form, please call 020 7811 6400.

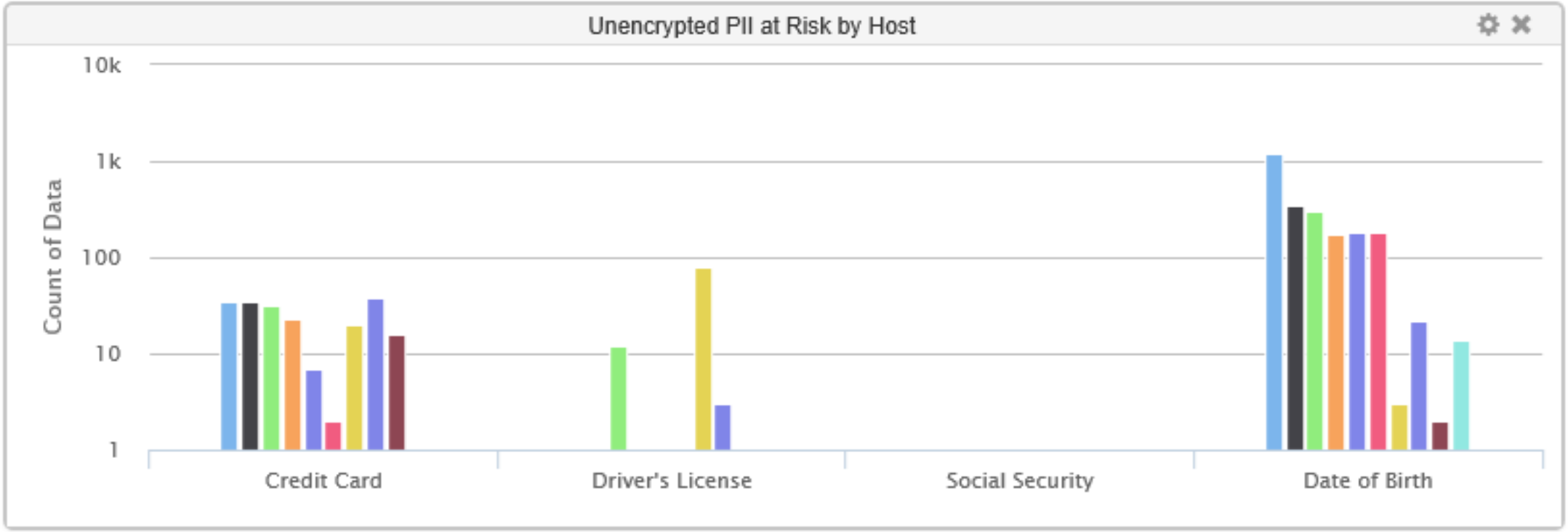
Data Protection

IPSA will process the personal information you provide and the personal information it obtains, for the purposes of exercising its statutory functions and as set out in the IPSA Freedom of Information and Data Protection Policy. IPSA may disclose information to third parties where it is required or permitted to do so by law. IPSA is a public authority under the Freedom of Information Act 2000 (FOIA). The information it holds may be disclosable under FOIA. Under the Data Protection Act 1998, you have the right to request a copy of the personal information which IPSA holds on you. To make a request, please contact IPSA's Data Protection Officer. IPSA may charge the statutory fee for access. For further information about how IPSA processes your personal information, please contact IPSA's Data Protection Officer at IPSA, 4th Floor, 30 Millbank, London. SW1P 4DU.

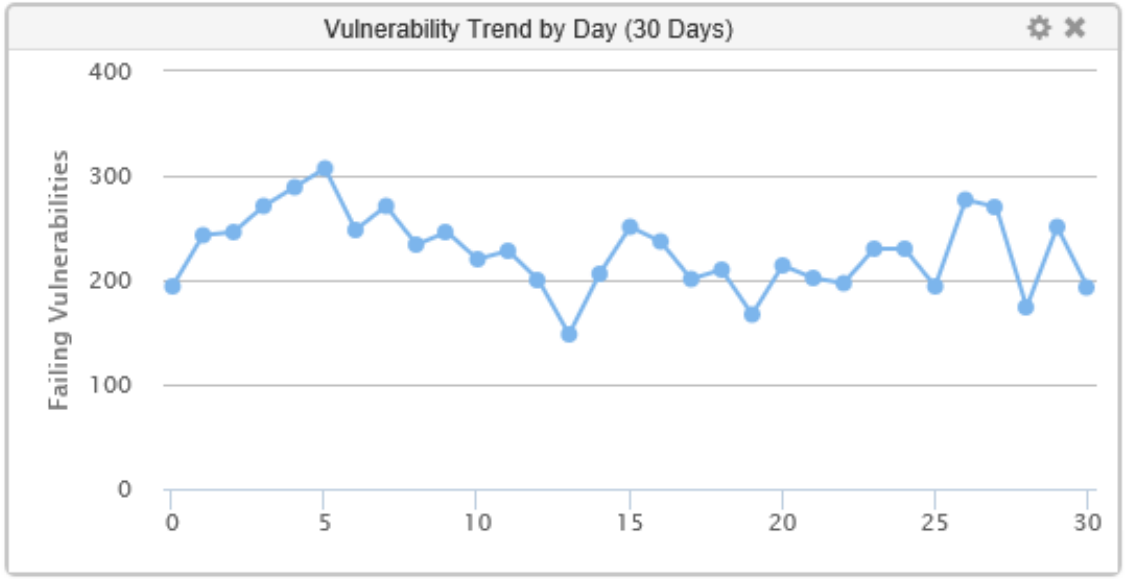
New Starter and Leaver Forms

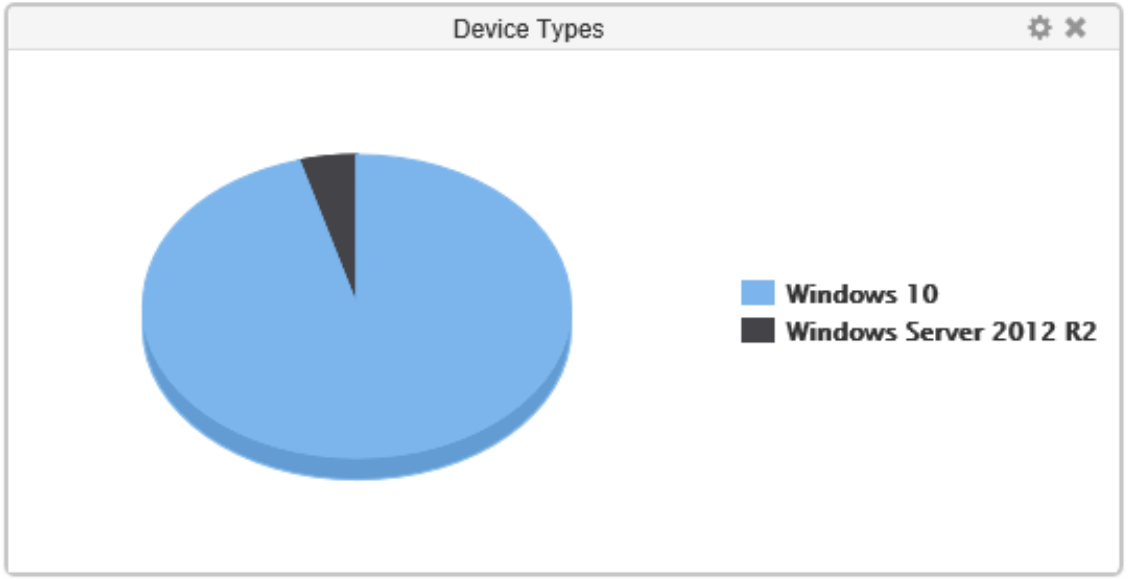


Risk Intelligence Tools



Risk Intelligence Tools





Risk Intelligence Tools

My Recommended Products and Services

Malwarebytes | ENDPOINT PROTECTION

Bitdefender

Managed Online Backup

Acronis Backup

4
Anti Malware

Executive Summary Report

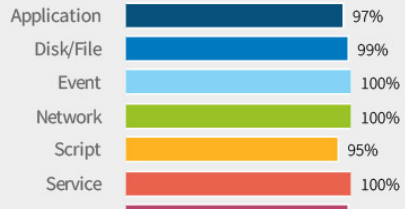
Health Score

Proactive Monitoring	100%	Server Availability	94.5%	Failed Login Attempts	0.5%
Antivirus	88.8%	Patch Management	56.1%	Web Protection	50.3%
Coverage	80.1%	Coverage	98.1%	Coverage	0.6%
Protection	97.4%	Protection	14.1%	Protection	100%
Backup	85.3%	Closed Help Desk Tickets	82.7%		

Managed Devices

Devices

Checks Passing



Alerts Resolved

4890

Remote Monitoring & Patch Management Tools

My 5 Steps (+2) to Securing your Data (Cybersecurity)

1 Boundary controls

Protect the online doors and windows of the business. Firewalls prevent unauthorised access from the Internet and are an important control. Password protect wireless (WiFi) and avoid using public wireless for confidential business actions.

2 Access Control

Restrict access to valuable data and systems. Make sure accounts are cancelled when employees leave the company. Log out from computers when stepping away and monitor accounts with special permissions such as administrator accounts.

3 Secure Configuration

Using applications as they come 'out of the box' can be unsafe. Secure configuration is about limiting the opportunities for the attackers. Disable unused accounts and services. Use strong passwords and back up your data regularly.

4 Anti Malware

Anti-malware scan computers looking for malicious files and program behaviour. Make sure anti-malware is installed and set automatically check for updates to protect against your threats.

5 Patching

Stay safe by keeping systems up-to-date. Hackers target old and vulnerable systems. Patching can ensure automatic updates are enabled, including web browsers. Delete all programs that are not required for work.

6 Education

Fact.. Hackers will target users as they are typically the weakest part of the system.

Solution.. Provide regular training and briefings to staff on how to protect themselves online.

"Don't learn the hard way!!"

7 Incident Planning

Fact.. Hackers will rely on the fact that their targets will have not planned for the attack.

Solution.. Reduce the impact of the attack by having a plan in place to activate.

My Recommended Services

Microsoft Azure

Office 365

Windows 10

ENTERPRISE MOBILITY + SECURITY

My 5 Tips to GDPR Compliance

Assess	Assess your current Cybersecurity status and get board level buy-in to facilitate change.
Conduct	Conduct an Information Audit of all data you hold and ensure personal data is properly classified.
Deploy	Deploy tools such as RMM, Patch Management and Risk Intelligence to proactively monitor your systems.
Remove	Remove legacy IT systems and employ up-to-date/compliant systems such as the Microsoft cloud, where possible.
Assess and refresh	Regularly assess and refresh your IT policies and processes such as your Information Security Policy, Password Policy, Right to be Forgotten process etc and provide clear training to all staff.

Many thanks for attending today!

GDPR – An IT Guide To Protecting Your Data

by Kris Daniels, Solve-IT