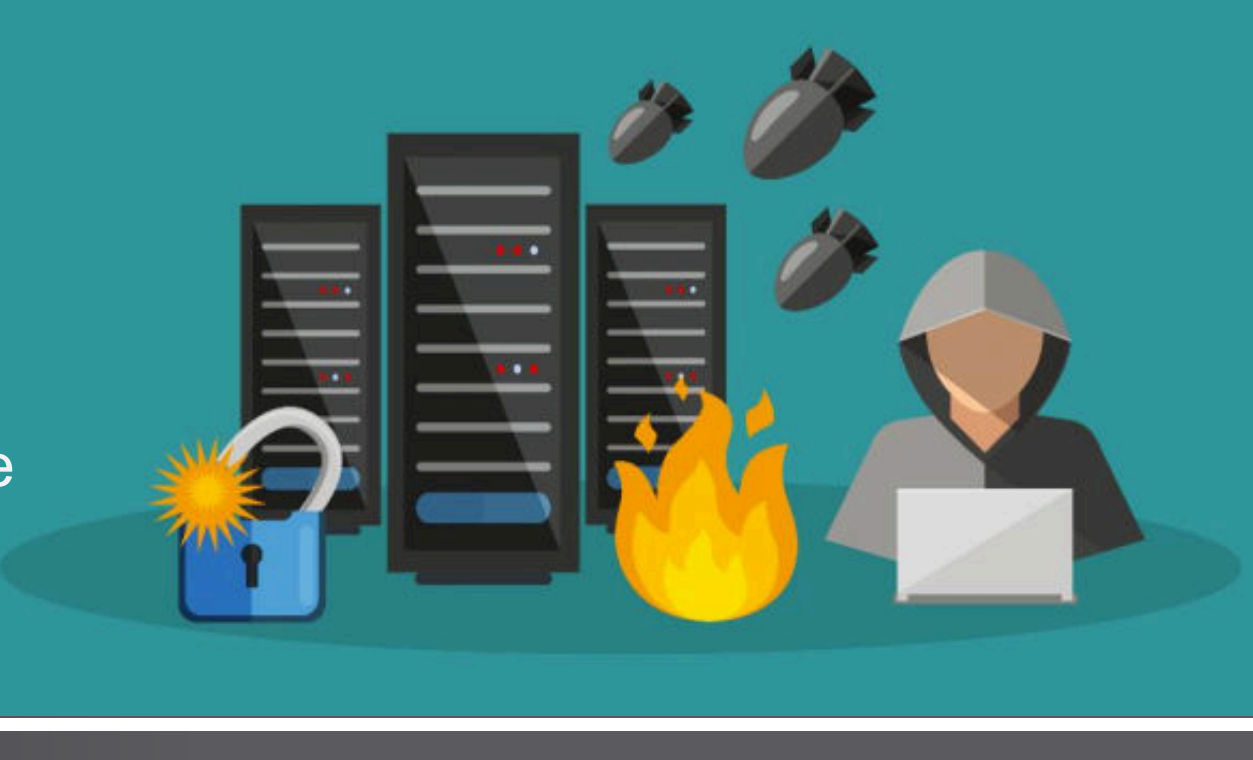
Is your network under attack?

The connections from your networks to the Internet and other partner networks expose your systems and technologies to attack. Reduce the chances of these attacks succeeding or harming your organisation.



Network versus application attacks [1]

Applications and networks present risks. Criminal hackers could gain access to sensitive information inside the network or inside applications that have access to the network.

Network	Application
64%	63%
of organisations experience a network attack vector	of organisations experience an application attack vector

Common types of network attack

- Eavesdropping
- Data modification
- Identity spoofing
- Password based
- Denial-of-service
- Man-in-the-middle
- Compromised key
- Sniffer
- Application-layer

What are the risks?

Networks need to be protected against both internal and external threats. Organisations that fail to protect their networks appropriately could face a number of risks, including:

Exploitation of systems
An attacker can compromise systems that perform critical functions.

Compromised information
An attacker can access systems hosting sensitive information directly or intercept information while in transit.

Insertion of malware
An attacker can import malware with the potential to compromise business systems, or release malware externally with associated reputational damage.

Denial of service
An attacker can deny access to services and resources to legitimate users or customers.

Damage or defacement
An attacker can damage internal and external facing systems and information.

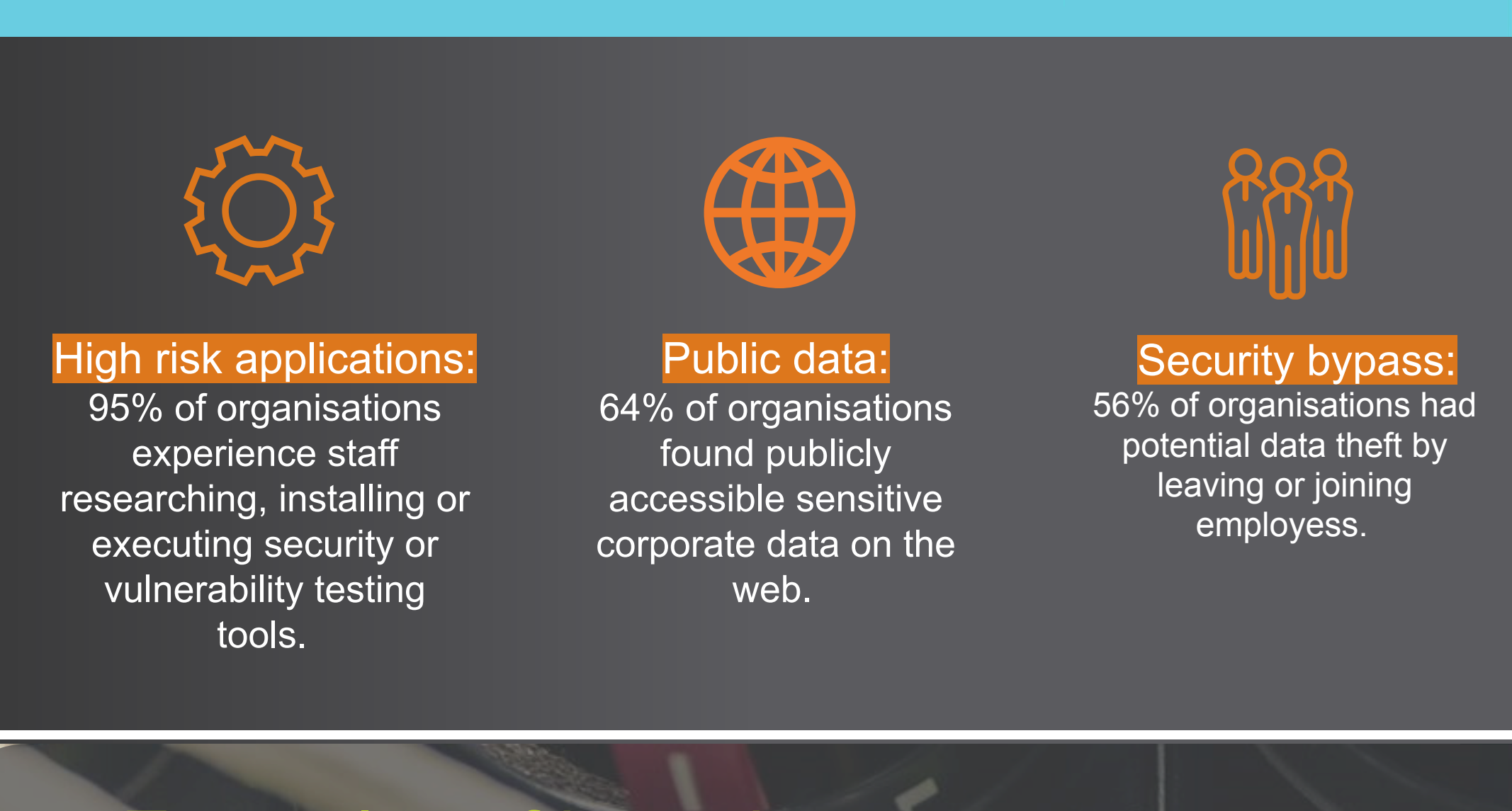
Where are the vulnerabilities? [2]

Internal networks reveal far more vulnerabilities than external networks. Internal networks often have rogue services running, and many devices lack basic host-based firewalls or endpoint solutions.

Engagement type	Percentage of engagements revealing at least one vulnerability	Percentage of engagements revealing at least one misconfiguration
External (web, phishing, VPN etc)	42%	55%
Internal (connected, physical, Wi-Fi etc)	96%	96%
Mixed engagements	83%	83%

The insider threat [3]

Internal users have already bypassed many physical controls designed to protect computer resources. This means organisations need to take further steps to protect themselves from the internal hacker threat.



MALICIOUS USERS
Users who intentionally harm the company. These are employees who steal sensitive data, intellectual property, client lists etc. They can also be disgruntled saboteurs.

NEGLIGENT USERS
Users who cause security breaches by accident. These users unintentionally risk security by misunderstanding security practices, or through human error.

INFILTRATORS
Outside attackers who infiltrate your organisation. These include hackers, credential thieves etc. who are operating as an insider within the organisation.

High risk applications:
95% of organisations experience staff researching, installing or executing security or vulnerability testing tools.

Public data:
64% of organisations found publicly accessible sensitive corporate data on the web.

Security bypass:
56% of organisations had potential data theft by leaving or joining employess.

Examples of breaches

Bupa employee stole half a million customers' health insurance data [4]

In August 2017, Bupa admitted that one of its employees stole information relating to 547,000 customers. The data included names, dates of birth, nationalities and some contact and administrative information. It's not yet known why the employee took the data, but common motives are financial gain (by selling the data to other criminals) and revenge (to disrupt business and cause reputational damage).

Former sysadmin installs malware time bomb [5]

In April 2017, Allegro MicroSystems filed a lawsuit against a former systems administrator who allegedly installed malware on the company's network. The employee resigned from the company in January 2016, but is accused of returning to Allegro's premises three weeks later to install a malware time bomb that would eventually cost Allegro a reported $100,000 in damages.

Uber suffered a massive data hack [6]

Uber hid a massive hack that resulted in cyber thieves pilfering the personal information of 57 million customers and drivers. Attackers accessed a GitHub coding site used by Uber software engineers, found a set of login credentials, and used those credentials to access an infrastructure account that handled computing tasks for the company.

Ukranian blackout blamed on cyber attack [7]

A recent attack on Ukraine's national grid that left 225,000 homes without power, which started with a phishing email. From that foothold, hackers were able to gain remote access to the network - including the highly specialised industrial control software that gives operators remote command over equipment like circuit breakers.

Network penetration testing

Network testing can help security professionals gain insight into where and how to invest their limited resources. Penetration testing may be required because of regulatory compliance, due diligence or contractual obligations, or it may simply be because of concerns that network controls are not properly implemented.

External penetration testing
Focuses on the organisation's boundaries – how it connects with the Internet and other external systems. If the systems are not designed correctly, this creates a perfect loophole for hackers to enter a network.

External penetration testing (customer-level access)
Establishes whether unauthorised access can be gained via the external network with the same level of access as your customers and suppliers.

Firewall and security systems
Assesses the effectiveness of the policies employed by your firewalls and the infrastructure in place for administration.

Internal penetration testing
Focuses on testing for vulnerabilities in systems that are accessible to authorised network connections (or login IDs) that reside within the network domain of the organisation.

Choose which test you need

At IT Governance we offer two levels of penetration test to meet your budget and technical requirements.

Level 1

Identifies the vulnerabilities that leave your IT exposed. Combining a series of manual assessments with automated scans, our team will assess the extent of your system or network's vulnerabilities, allowing you to evaluate your security posture and make more accurate budgetary decisions.

Purchase our quick and fixed-price penetration tests online.

Buy online

Level 2

Involves attempting to exploit the identified vulnerabilities to see whether it is possible to access your assets and resources. This more thorough assessment of your security posture enables you to make more accurate decisions about investing in securing your business critical systems.

Please contact us for further information.

Contact us

For more penetration testing information or to request a quote, visit our website by clicking here.

References

1. Pick Your Poison: The Most Popular Cyber-Attacks of 2016, Radware (2017).
2. Under The Hoodie: Actionable Research from Penetration Testing Engagements, Rapid 7 (February 2017).
3. Insider Threat Intelligence Report, Dtex (2017).
4. Bupa Employee Stole Half A Million Customers' Health Insurance Data, DigitalHealth blog (July 2017).
5. Former sysadmin installs malware time bomb, IT Governance Blog (May 2017).
6. Uber hid massive hack compromising data of 57M for a year, SC Media (November 2017).
7. Ukranian Blackout Blamed On Cyber Attack, Telegraph (June 2017).