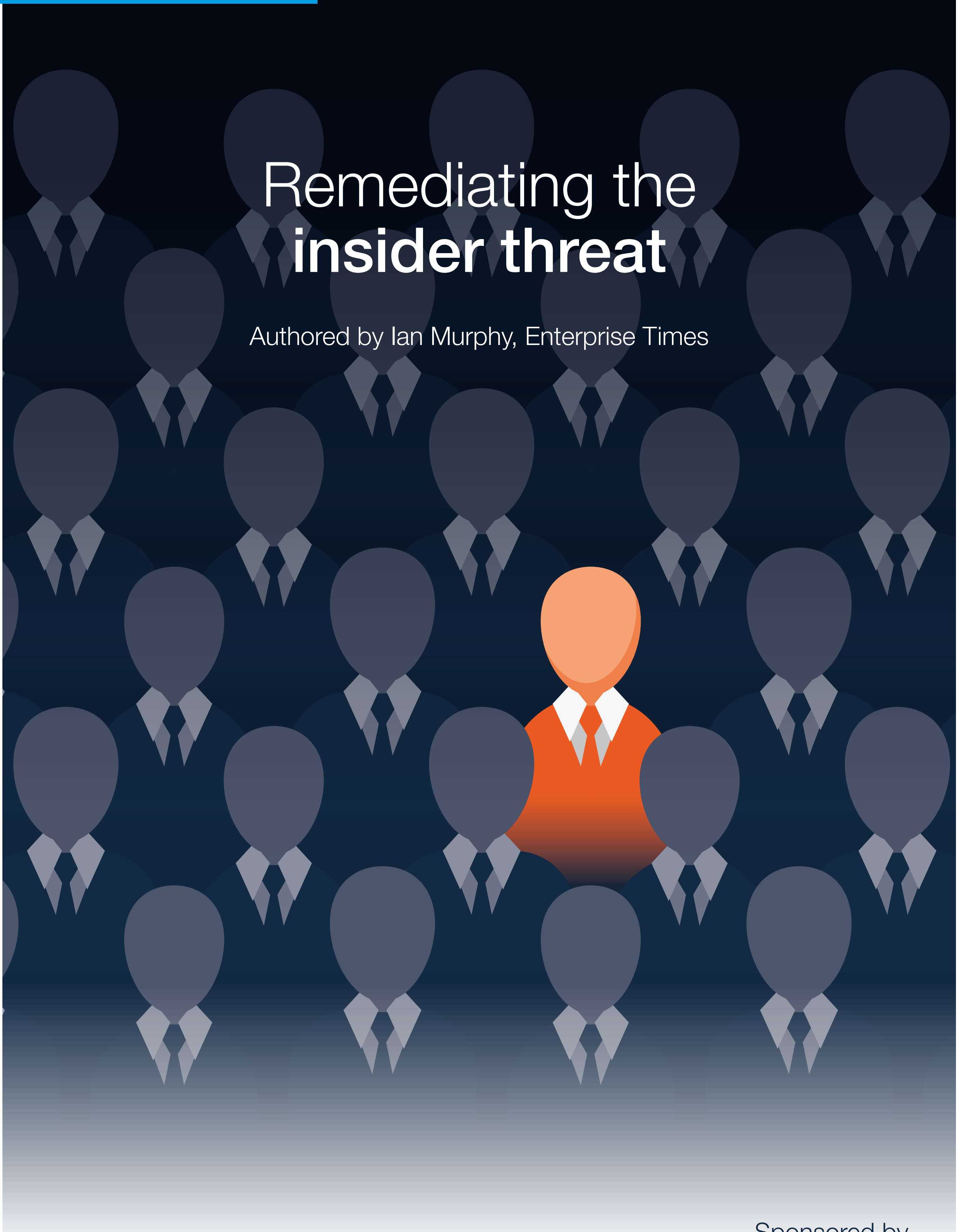
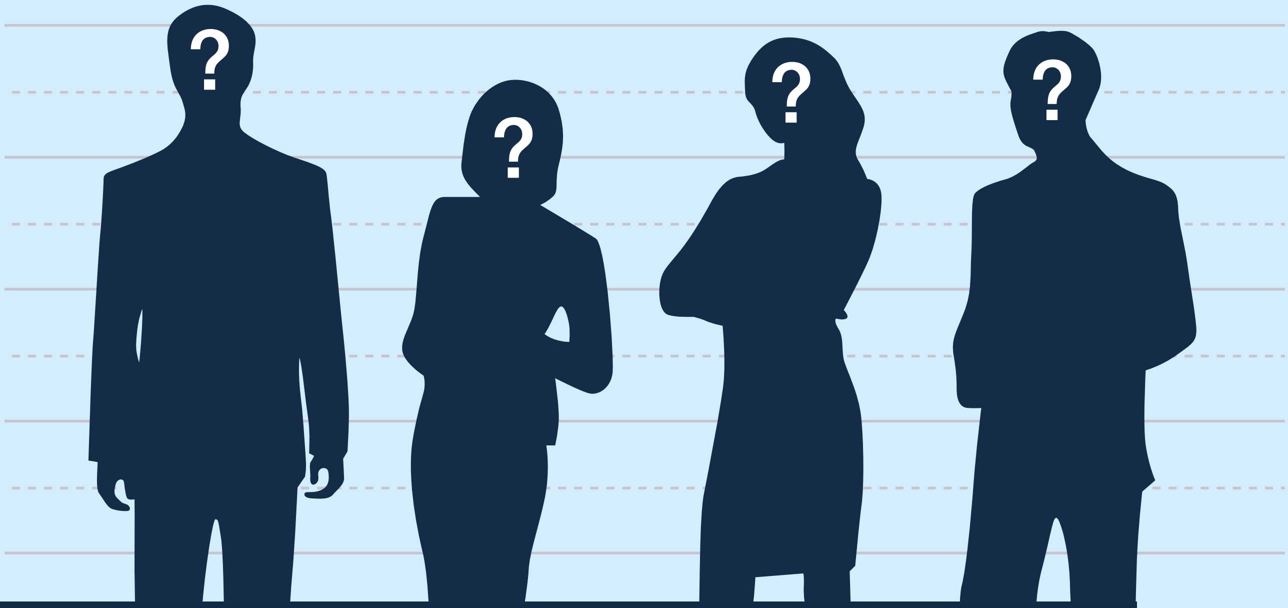
INDUSTRY WHITE PAPER

Remediating the **insider threat**

Authored by Ian Murphy, Enterprise Times



Sponsored by



The Insider Threat is a significant challenge for organisations at many levels. It raises issues of trust between the business and its employees, contractors and partners. It is something that is not only difficult to spot but is capable of causing serious damage to a business both financially and reputationally through data breaches and the associated fines.

Whilst trying to mitigate the risk of an insider breach, the most important thing to accept in any approach to data security is that there is no-one-size-fits-all solution. There is also no single approach that fixes everything. To address security issues, organisations need a blend of education, people, process and technology.

None of this is new to Chief Information Security Officers (CISOs) or any other person accountable for managing cybersecurity and data risk. Businesses have poured, literally, billions of dollars into dealing with cybersecurity. Industry analyst Gartner claims that around US $100 billion was spent in 2017 on buying information security technology solutions. In 2018 that was expected to rise to over US $114 billion and will continue to grow. Other analysts report similar spending levels.

Many organisations should ask themselves three questions when the subject of insider threat comes up:

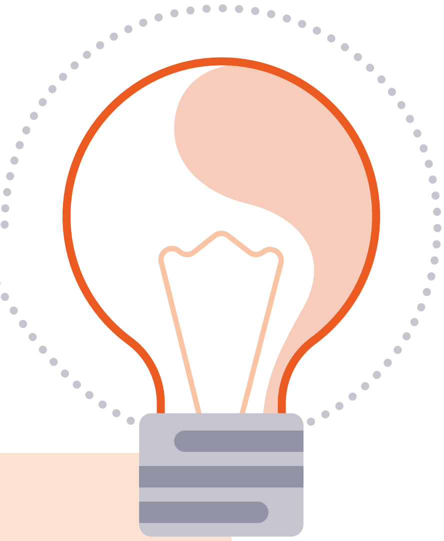
1. What damage can the insider do?
2. Who are they?
3. How do we protect the business or organisation against them?

The damage to the organisation

There are many ways that the insider can damage the business. Take the case of Edward Snowden. His theft of confidential and secret military data is still causing problems for the US military and its intelligence services. Snowden, like many insiders, didn't hack into any systems, he just copied data that he had access to.

Andrew Skelton was an internal auditor at UK supermarket chain Morrisons. This meant that he legally had access to a lot of personal data on employees. When he was accused of dealing legal highs at the company, Skelton leaked the details of over 100,000 employees on the web. The resulting damage has seen Morrisons ordered to compensate employees, past and present, even though it was not directly responsible for the actions of Skelton.

In January 2019, the FBI charged Jizhong Chen, a Chinese national, with stealing trade secrets from Apple. Chen worked on Apple's self-driving car project and is believed to have stolen key intellectual property which he intended to take with him to China. Chen had access to the data as part of his role in the company.



A user sends an email with Personally Identifiable Information (PII), say payroll data, to the company payroll processor. Unfortunately, they type in the wrong email address or autocorrect in the email client inserts the wrong address. The result is that data ends up going to the wrong person, often external to the company, risking a fine of significant proportions under GDPR.

Who are the insiders?

All of the above data breaches were caused by users with lawful and reasonable access to the data. One claimed moral imperative, one acted out of spite, one was motivated by financial gain and one made a mistake. All of these are different types of insider threat that have to be guarded against.

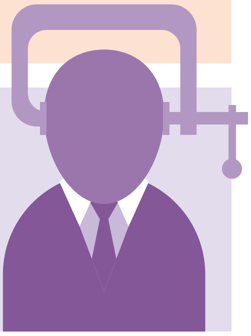
In defining the insider threat, there are five primary categories:

Criminal

This insider sets out to steal, damage or destroy data often for financial gain. They often target intellectual property (IP), customer lists or financial data. The case of Jizhong Chen above is an example of a criminal attacker.

Emotion-driven

These are people who believe that the company or another employee has wronged them in some way. Both Andrew Skelton and Edward Snowden fall into this category. They both had issues with their employer and chose to steal and release data.



Pressured

Debt and activities outside of work such as criminal or embarrassing behaviour are often the root cause for those pressured into helping criminals steal data.

Negligent

This is a set of employees who refuse to change risky behaviour. It might be the sites they visit, constant movement of company data to insecure cloud services or regularly clicking on phishing emails.

Accidental

Employees who fall for a well-crafted spear phishing attack or inadvertently sends sensitive data to the wrong person via email.

There are several steps that organisations can take to reduce the impact of the insider threat. Each one has an impact on a different group of attackers. They break down into three groups: technical solutions, improved process and practises, and education.

Strategies for remediation

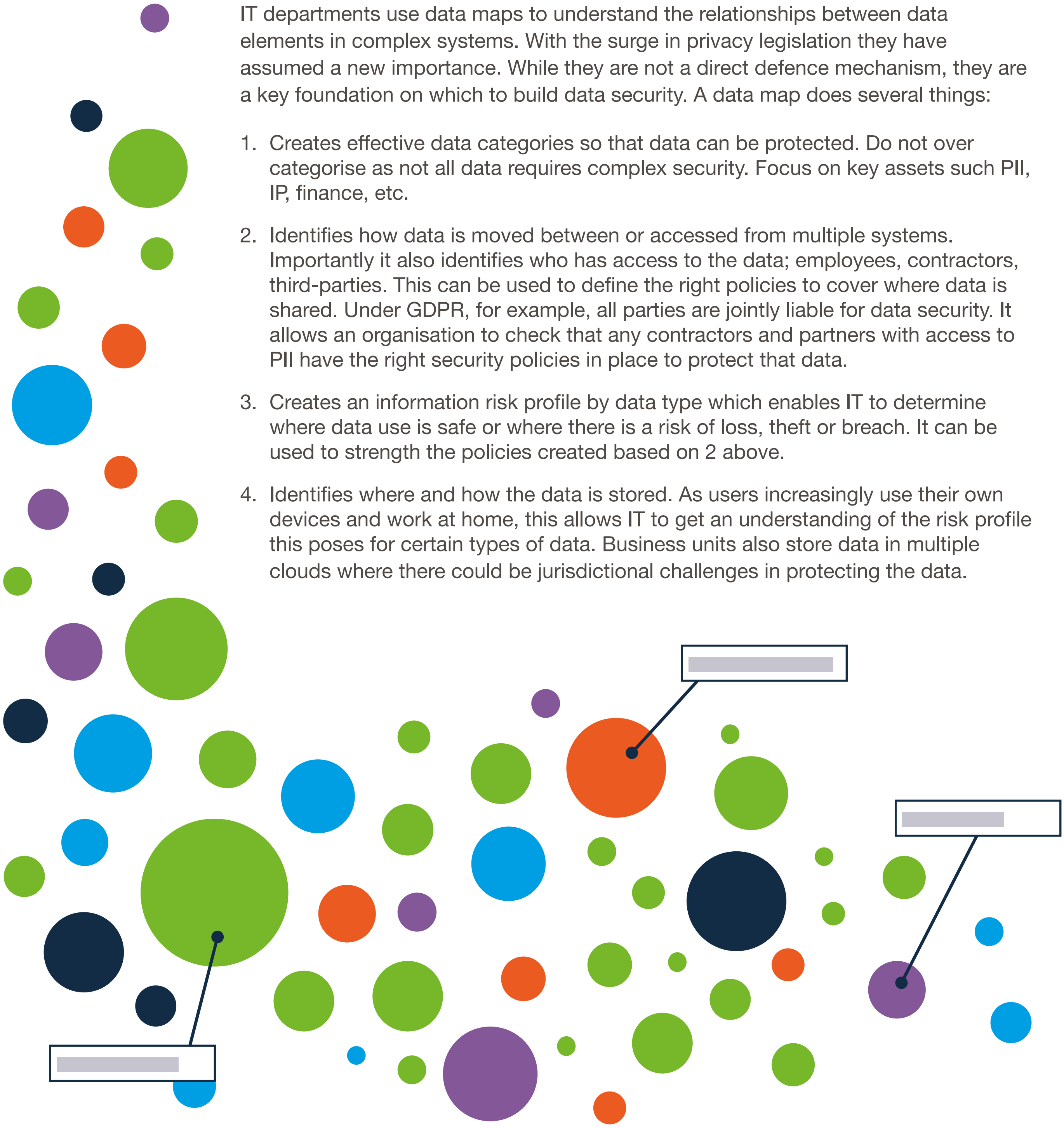
Technical solutions

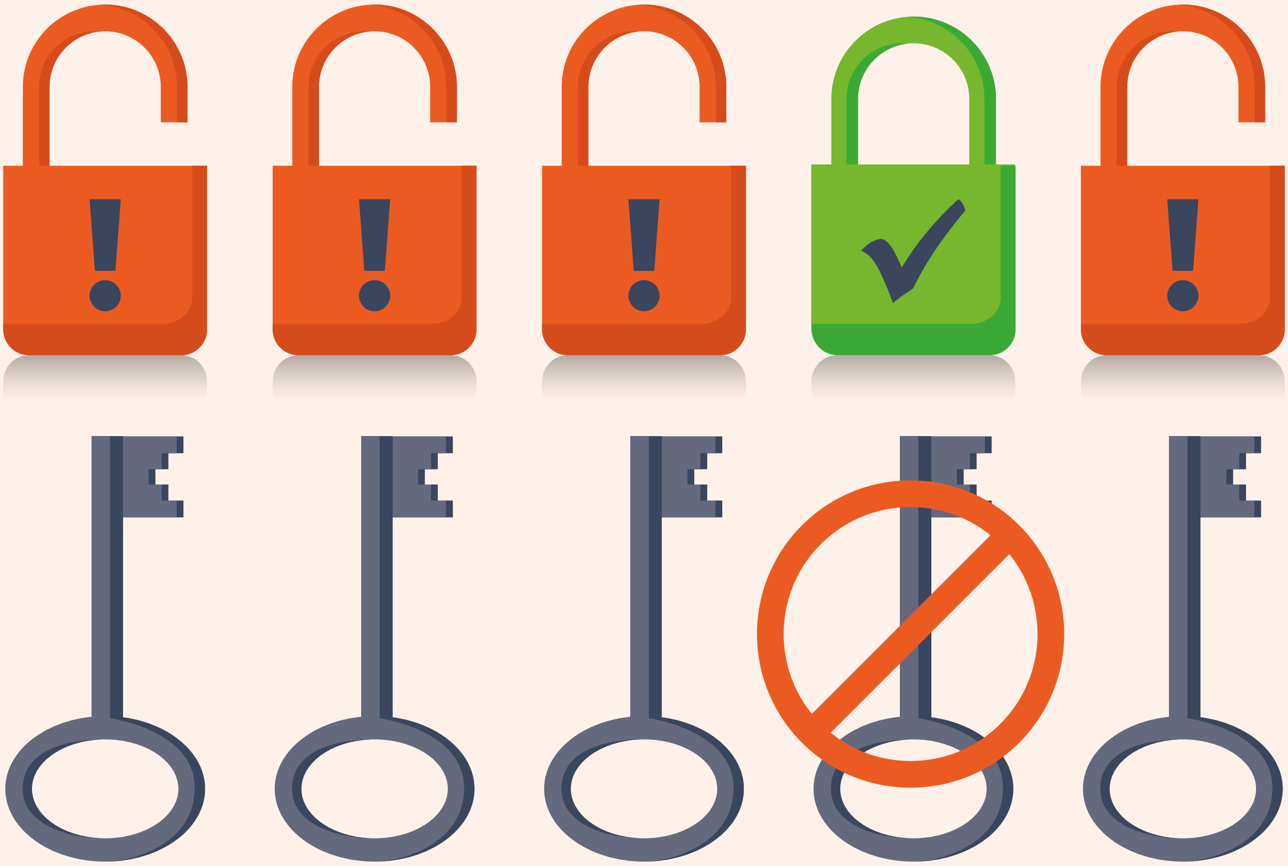
There are a number of technical solutions that an organisation can put in place to help spot the risk of an insider threat. Many of these will also help spot other attacks from hackers. Here are some of the most effective.

Data maps

IT departments use data maps to understand the relationships between data elements in complex systems. With the surge in privacy legislation they have assumed a new importance. While they are not a direct defence mechanism, they are a key foundation on which to build data security. A data map does several things:

1. Creates effective data categories so that data can be protected. Do not over categorise as not all data requires complex security. Focus on key assets such PII, IP, finance, etc.
2. Identifies how data is moved between or accessed from multiple systems. Importantly it also identifies who has access to the data; employees, contractors, third-parties. This can be used to define the right policies to cover where data is shared. Under GDPR, for example, all parties are jointly liable for data security. It allows an organisation to check that any contractors and partners with access to PII have the right security policies in place to protect that data.
3. Creates an information risk profile by data type which enables IT to determine where data use is safe or where there is a risk of loss, theft or breach. It can be used to strength the policies created based on 2 above.
4. Identifies where and how the data is stored. As users increasingly use their own devices and work at home, this allows IT to get an understanding of the risk profile this poses for certain types of data. Business units also store data in multiple clouds where there could be jurisdictional challenges in protecting the data.





Improve access controls

One of the biggest challenges for organisations is managing effective access control to data. This is not due to a lack of technology but because access rights bloat over time. Three examples:

- A member of the HR team moves from one division to another division inside a large multinational company. They should no longer be able to access the PII of the former division.
- In multinationals it is common for fast-track executives to spend time in different functions such as procurement and production. As they change roles, if those roles are no longer related to the previous division, they should no longer be able to access data.
- An individual is transferred from the IT support role for the commodities team in a brokerage to a more senior IT support role for the derivatives team. Under compliance rules, they cannot retain any access to the commodities floor or systems.

> "In most organisations, access rights to the systems they used in previous roles are rarely revoked quickly, if at all."

In most organisations, access rights to the systems they used in previous roles are rarely revoked quickly, if at all. During that time, the employee is at risk of becoming a security risk as any breach of their identity credentials could reveal highly sensitive data.

This is a common problem across organisations that needs to be addressed. It is not simple but the approach to take is one of least permissions. This could be initiated by HR who know about the change in role and responsibilities. Alternatively, it can be dealt with through regular reviews of permissions and access to data.

Analyse logs and user behaviour

One of the major growth areas in security has been better use of analytics. Machine learning solutions make it easier to import very large amounts of data from log files and find anomalies. These can then be referred to a security analyst for more detailed analysis. One of the key elements to making any analytics effective is context.

Typical context markers are:

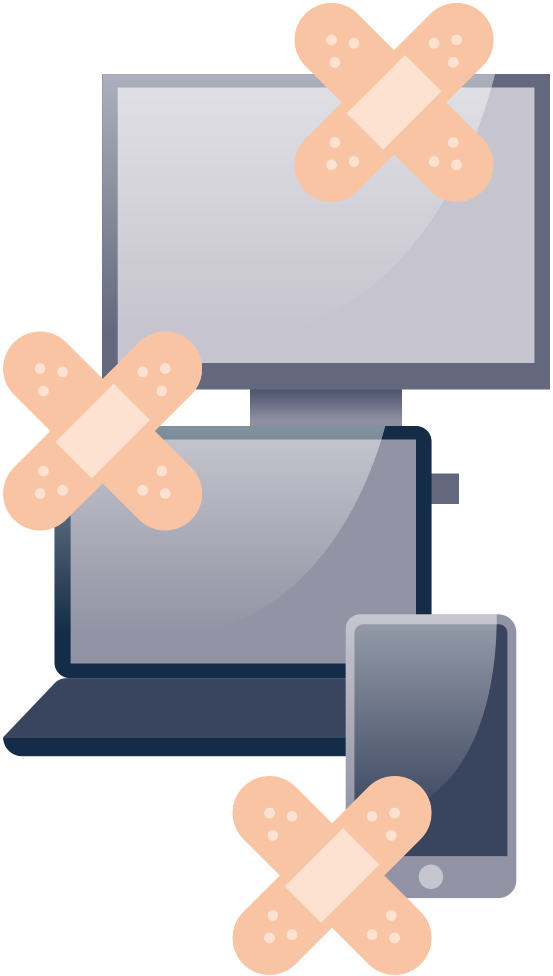
- Does the user have the right permissions to access the files?
- Where were the files accessed from?
- What date were the files accessed?
- What time were the files accessed?
- Are both of the above consistent with the working day in the location where they were accessed from?
- Does the employee accessing the files use a VPN?
- Is this a data location that the employee has access to but has never, or very rarely, accessed and is now accessing often?

Context can be useful in deciding to take further action or ignore. If a log file flags that data belonging to the finance department has been accessed from Japan, the context data could be:

- The corporate calendar, shows that the CFO is in Japan talking with a major shareholder. It is reasonable, therefore, that they have accessed those files.
- The data and time of access are early in the morning and the company has nobody in Japan. Lock the user account and track all data accessed by those credentials. Contact the user to ascertain if they have been compromised.

While the second action might cause some embarrassment, it is better than having stolen credentials used to steal data.

Much of this context checking can be done automatically and further reduces the load on the security analyst. However, there are times when this will fail. Take the access control challenge above. One of the easiest ways of detecting an unauthorised attempt to access data is by checking if the individual has the right permissions. If they do, most systems won't even flag up the access let alone prioritise it.



Patching, security alerts and protecting end user devices

Frustrating the attacker is about raising the bar and making an attack more difficult. This is as true for the external attacker as it is the insider. The challenge with the insider is that they are inside the hard shell of the enterprise. However, many attacks enabled by insiders are because they allowed an attacker a foothold in the first place. This is typically by falling victim to a spam, malware, phishing or drive-by attack.

One solution, as discussed, is to better educate the user. Another is to ensure that all devices, servers, systems and services are promptly and properly patched. As many times as this is said, every year the list of known and successful attacks show that many attacks rely on old, well-known, vulnerabilities.

When it comes to end user devices, the problem is more complex. Bring Your Own Device (BYOD) relies on end users making the capital investment in technology rather than the employer. Before devices are connected to the network and used to access data they should be checked to see if they are properly patched. If not, helping staff patch and maintain their devices is a sensible move.

Another is to extend access to software licences for end user security products and core applications such as Microsoft Office. If the users have access to the same software across all their devices they are unlikely to use less secure or unknown software. It allows IT to check patching and security levels and advise users accordingly.

Protecting shared data

Whether intentional or accidental, one of the greatest areas of risk for any businesses is when potentially sensitive information is shared externally.

By encrypting data from end-to-end, users can ensure that information is delivered securely and track access through reporting and audit logs. In addition, some solutions offer real-time revocation, but on their own, they don't necessarily mitigate the risk of an accidental or malicious send.

Instead organisations need to consider technologies that also leverage behavioural analytics and machine learning to interpret sharing patterns, relationships, domains and data to identify when things don't look right and then prompt either the user or the admin to take action. These technologies can also be used to automate decisions that often fall foul of human error and subjectivity, such as when to apply encryption.

Improved processes

A simpler reporting process

Reporting a cybersecurity incident can be complicated in many organisations. That complication often leaves users feeling that the time required to report an incident is not worth the effort. The amount of information that security teams ask for before they look into an incident can also be an inhibitor to reporting.

For the accidental and negligent insider, as well as other users, a simpler web-based reporting process that requires less than a minute to complete will help reduce the impact from insider threat.

No fault reporting

In addition to simplifying the reporting process, organisations need to consider introducing no-fault reporting. If a user thinks that a report will cause them problems inside the business, they will not make the report. It has a direct impact on the accidental and negligent insider. If backed up with improved education and other approaches, it will harden not weaken security. It also engages staff in becoming the first line of defence.

> “In addition to simplifying the reporting process, organisations need to consider introducing no-fault reporting.”

Ensure security policies deal with internal and external staff

One of the challenges of security is that organisations are becoming increasingly integrated. Access to systems and data is by employees and external contributors, such as contractors, who may also work for partners or competitors. Another is the use of collaboration software and the encouraging of employees to share data with key business partners, suppliers and customers. All of these allow third-parties access to company data. In addition, organisations often share data they have collected with third-parties as part of a revenue scheme.

GDPR has expanded responsibility for data ownership. Where data is shared, all parties are jointly liable for its security and safety. For example, a doctor’s surgery shares the details of its patients with a key drugs company to help them develop new drugs. A laptop belonging to that drugs company is stolen with the data on it. Both the surgery and the drugs manufacturer are jointly liable for the data loss under GDPR.

This also extends to employers being liable for actions carried out by their employees. For example; in the case of supermarket chain Morrisons, where a disaffected employee published PII for staff online. The courts held that Morrisons had to pay compensation to staff for the data breach.

Where data is shared, an organisation should ensure that it understands the data security processes of the partner. It needs to undertake a risk assessment to ensure that the data is going to be protected. An insider breach at the partner has the same implications as a breach at the company that has collected the data. This means requiring partners to provide copies of their own processes for data protection and ensuring that they are good enough. It is also reasonable to check that those processes and policies have been implemented

Education

As with most initiatives, it starts with educating users. Organisations have been doing this for some time with variable effects. Some do annual training where users spend a day learning about cybersecurity threats. It's an approach that works well for fire-fighting, first aid and child protection but does not work for a constantly changing threat such as cybersecurity.

Education needs to be a constant feed but not intrusive. Here are some simple approaches:

Intranet

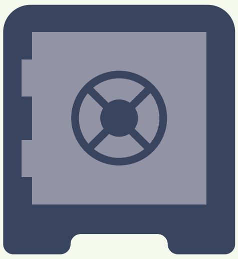
Use the company intranet to post examples of cybersecurity threats. List out the different threat types and how to spot them such as spam, phishing, malware attachments. For example, with email threats post the latest examples that have been spotted on the email server, what users should look for and how to easily identify them.

Testing and gamification

To test if users can spot phishing or spam emails that get through the email server, IT security sends fake phishing emails to users. It monitors user reaction to the email. Do they click on links? Delete the email? Use internal reporting approaches to notify IT or other members of their team? By adding in a reward option – perhaps the best performing person/department is given extra time off or maybe a small bonus payment – this can drive user interaction.

Understanding sensitive data

Ensure users are aware of the data classifications in use and how to identify sensitive data. This is particularly relevant for those handling PII both internally and when they are dealing with partners. Staff who collaborate with people inside and outside the business need to understand that not all data is freely sharable. It is essential that know how to seek advice on what to share and what to not share.



Safe storage of data

The increased use of cloud services and shared document libraries means that users need to be aware of how to store data safely. IT needs to make sure that users have access to approved secure cloud storage that can be used for storing company data. This should be part of a rolling programme and include training on other software packages.

Conclusion

There is no single set of data security solutions, set of processes or education that can make everything safe. What is important is that the approaches taken are integrated and can cover both insider and external threats.

For the different types of insider threat identified here, the key solutions outlined help by reducing the risk. The solutions and how they address insider threats are:

Criminal

Data maps, improved access controls and better analytics of both log files and user behaviour.

Emotion-driven

Data maps, improved access controls and better analytics of both log files and user behaviour.

Pressured

Data maps, improved access controls and better analytics of both log files and user behaviour.

Negligent

Improved access controls, better analytics, simpler reporting processes, education and, where necessary, reporting processes managed by HR. Install and monitor security solutions to protect and prevent malware on local devices

Accidental

Education, simpler reporting, no-fault reporting and the use of security solutions to protect and prevent malware on local devices

There are other approaches that organisations could take but the key with those listed here is that they can be deployed without being intrusive. Intrusive security is always self-defeating. If it prevents users doing their job, they will find a work around. It doesn't matter whether it's the applications, devices, storage or the data. The ingenuity of users to find the easiest path is well proven.

> "Intrusive security is always self-defeating. If it prevents users doing their job, they will find a work around."

Stopping the insider attack is about deploying the right mix of education, process and technology. We have looked at some of the approaches that organisations can deploy with little additional overhead to time, budget or working practice. All of these will help reduce the risk from the insider, making the company, and its data, a little more secure.

Enterprise Times

Enterprise Times delivers a mix of news, features, blogs and podcasts covering the information technologies used by enterprises. Their editorial team has over 75 years of experience both as practitioners and writing about the changes in the technology market.

enterprise times

Egress Software Technologies Ltd

Egress Software Technologies is the leading provider of privacy and risk management services designed to manage and protect unstructured data in a seamless user experience.

The Egress platform leverages machine learning-led policy management, encryption and discovery to enable end-users to share and collaborate securely, while maintaining compliance and reducing the risk of loss.

www.egress.com

✉ info@egress.com
☎ 0844 800 0172
@EgressSoftware

egress®