Wilson James

Monthly Threat in Focus
February - Insider Threats

February - Insider Threat

1

Across the Industries

2

Types of Insider Threats

3

Facts and Figures

4

Mitigating against the Threat

5

Protecting Yourself

Advisory Services Monthly Threat In Focus:
Insider Threat – Across the Industries [1.] [2.] [3.]

Insider threats are those employees, contractors, service providers with legitimate access to a company's networks and systems who intentionally remove data maliciously and for personal gain or unintentionally share sensitive information

The sectors most likely to experience Insider Threat incidents are:

- Finance and Insurance.
- Government/Local Government.
- Entertainment.
- Information Technology.
- Healthcare.

The impact of an Insider Threat attack can be wide ranging from:

- Theft, deletion or tampering of sensitive data.
- Disruption to BAU.
- Reputational damage.
- Financial/regulatory costs.

Unintentional Insider Threats are the most common representing 86% of all incidents. **Intentional** Insider Threats represent 14% of incidents but can be particularly dangerous due to the privilege access the users typically hold.

Advisory Services Monthly Threat In Focus: Insider Threat - Types 4. 5. 6. 7. 8. 9.

TYPE	METHODOLOGY	CASE STUDIES
THIRD PARTY Intentional / Unintentional Act	**CONTRACTOR/VENDOR/ SERVICE PROVIDER** Contractors become a 3rd Party as they often will be required to use both their direct employers and/or their client Systems to manage client data.	**3RD PARTY HOSTING RED CROSS DATA – UNINTENTIONALLY SUBJECT TO A CYBER ATTACK** LOCATIONS AND CONTACT DATA ON 515,000 VULNERABLE PEOPLE STOLEN **Impact:** As a result of the breach the organisation shut down a program which aimed to reunite family members after conflict events resulted in them being separated, it is unclear if this is a temporary shut down or not at this time. **RED CROSS JAN 2022, (Reported by TECH CRUNCH.COM)**
CRIMINAL OR MALICIOUS INSIDERS Intentional Act	**COLLABORATOR** Insiders who abuse their legitimate access rights to access information and intelligence to share with a third-party **LONE WOLF** An insider who works independently and maliciously for their own benefit	
NEGLIGENT OR INADVERTENT USERS Unintentional Act	**GOOF** Insiders who intentionally or unintentionally cause actions that may cause harm often abusing security protocols **PAWN** Inside employees who are unaware, they are being manipulated into performing malicious activities	**GOOF INTENTIONALLY IGNORED SECURITY PROTOCOLS** BOEING EMPLOYEE EMAILED DATA TO WIFE'S PRIVATE ACCOUNT. **Impact:** 36,000 employee details where shared by email to the employee wife's private system. As directed by law BOEING reported the incident, the estimated Cost to the business was predicted to be approx. USD 5.7 Million. **BOEING FEB 2017 (Reported by REGISTER.COM)**

Advisory Services Monthly Threat In Focus: Insider Threat - Facts and Figures [10.] [11.] [12.] [13.] [14.] [15.]

THE PROBLEM

- **Only 42%** of companies have the **appropriate controls** in place to **prevent Insider Threats.**
- **27,000+ unauthorised emails** a year sent from 1,000+ employee companies in 2020.
- **Malware** is the most common form of cyber threat and **Crypto jacking** the least common.
- Only 2.3% of Twitter Accounts and 4% of Facebook Accounts use **Two Step Authentication** (2SA)
- **51%** of **businesses** have had a **data breach** due to a **third party**
- **55%** of **businesses** identify **privileged users** as their **greatest** insider **threat**

THE COST IN TIME AND MONEY

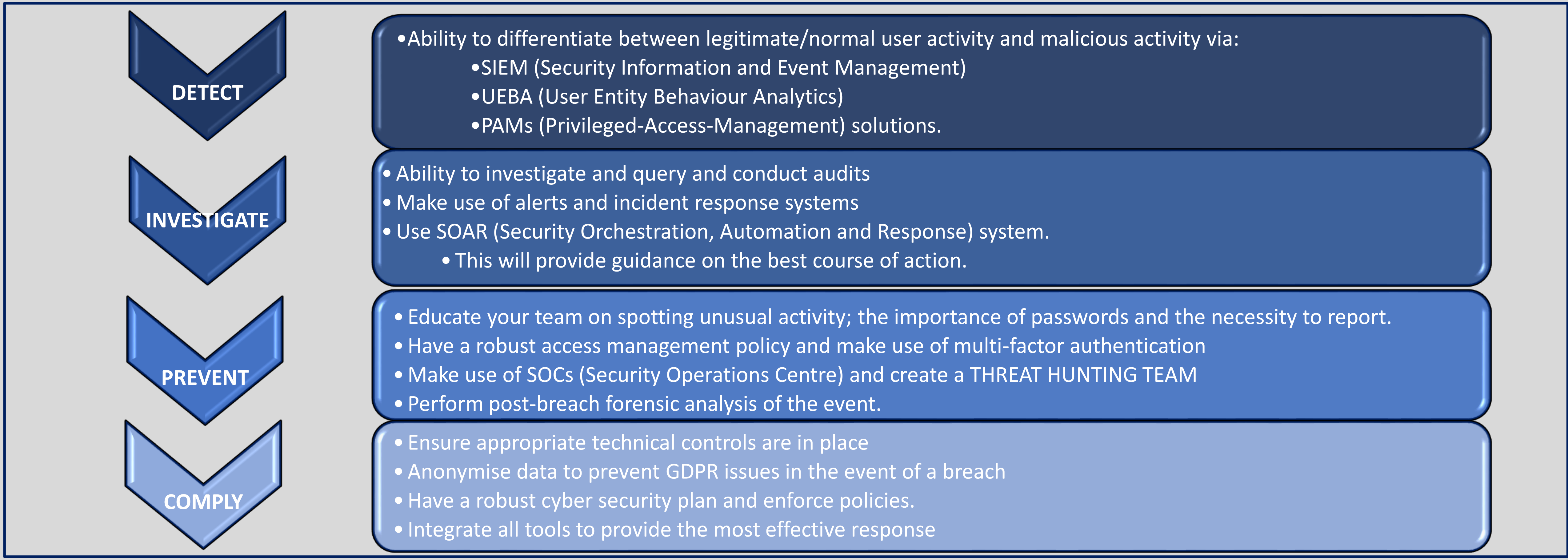
- **Average cost** of an insider threat in 2020 was **USD 11.45 Million**
- It takes on average **77 days** to contain an incident
- It takes on average **two months** to contain an Insider Threat

THE SOLUTION

- Google noticed **50% drop in hacks** after installing **two-step authentication** (2SA) as default.
- 61% of organisations in 2020 focussed on **prevention/deterrence** as a way of **combatting Insider Threat**

Advisory Services Monthly Threat In Focus:

Insider Threat – Mitigating against the Threat [16.] [17.] [18.] [19.] [20.]



DETECT

- Ability to differentiate between legitimate/normal user activity and malicious activity via:
  - SIEM (Security Information and Event Management)
  - UEBA (User Entity Behaviour Analytics)
  - PAMs (Privileged-Access-Management) solutions.

INVESTIGATE

- Ability to investigate and query and conduct audits
- Make use of alerts and incident response systems
- Use SOAR (Security Orchestration, Automation and Response) system.
  - This will provide guidance on the best course of action.

PREVENT

- Educate your team on spotting unusual activity; the importance of passwords and the necessity to report.
- Have a robust access management policy and make use of multi-factor authentication
- Make use of SOCs (Security Operations Centre) and create a THREAT HUNTING TEAM
- Perform post-breach forensic analysis of the event.

COMPLY

- Ensure appropriate technical controls are in place
- Anonymise data to prevent GDPR issues in the event of a breach
- Have a robust cyber security plan and enforce policies.
- Integrate all tools to provide the most effective response

Advisory Services Monthly Threat In Focus:
Insider Threat – Protecting yourself

USING DEVICES AT WORK

Managers - Ensure that any team members' systems/information access is appropriate for their role.

- Particularly where there is a change in position or when a team member leaves the business.
- Provide staff with personal account access.
  (Not one account username with multiple users.)

All Staff - Only share information when it is appropriate.

- Do not borrow colleagues' logons or passwords.
- Only click on links from trusted sources.
- Be aware of the company policy surrounding data sharing for both Wilson James and the client you are working for.
- Notify the appropriate Information Security Officer if you suspect inappropriate behaviour.
  - Who is the ISO when using a client system.
  - Who is the ISO when using a WJ system.

USING WORK DEVICES AT HOME

- Use the VPN provided by the business
- Ensure you shut down your device fully at the end of a day to enable updates to take place as required
- Do not use the same password for all devices linked to Wi-Fi
  - For example: Doorbell cameras or Virtual Assistance Devices

Sharing Data

- Do not send work emails to your personal email accounts.
- Do not download personal data from private email accounts on a works system.
- Only click on links from trusted sources.
- If required to share personal data ensure your using a registered and approved process as directed by your Information Security Team.

Reporting

- Notify the appropriate Information Security Officer if you suspect any phishing emails have arrived in your inbox.
- Notify the appropriate Information Security Officer if you suspect your system has become subject to a cyber attack.

Monthly Themes for 2022

1 Event Security- Crowd Management (January)

2 Insider Threat (February)

3 Social Media Auditors (March)

4 Activism (April)

5 Trespassing (May)

6 Fly-tipping (June)

7 Lone Working (July)

8 Scams (August)

9 Data Privacy (September)

10 Theft Property (October)

11 Terrorism (November)

12 Travel safely (December)

Advisoryservices@wilsonjames.co.uk