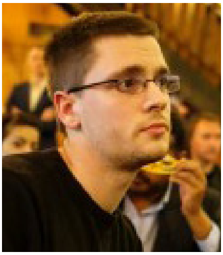

JOSEPH GOODY - *Lead Security Consultant, Cyberensic*
LinkedIn https://www.linkedin.com/in/joseph-goody-ed111111111/
Website https://www.cyberensic.io/

Joseph specialises in Cyber Security, focusing on innovative solutions to protect digital landscapes. With extensive IT experience, he crafts strategies against evolving threats, covering advanced networking, security protocols, and system optimisation. Committed to continuous learning and industry trends, he ensures top-notch service and security for clients. He is passionate about technology and problem-solving and leads his teams with excellence and proactive defences.

TIP 1. HONEY GETS YOU MORE THAN VINEGAR

Often, have I found that simply smiling and getting along with most people will lead them to tell you things about their work, processes, and procedures that they would otherwise be unwilling to disclose. If you want to find bugs/risks in your business, you'll get further with a teaspoon of honey than with a teaspoon of vinegar.

TIP 2. TAKING THE TIME TO PROPERLY THINK OUT RISKS

Most of, if not all the time I find when running Risk Reviews or Monthly Management Reviews things are often sped through, dismissed, or just plainly treated as a tick on the list of agenda items. Don't just discuss what could happen, go through how and why it would happen.

TIP 3. ELECT A DISSENTING PRINCIPLE

When starting up risk review, or any project for that matter, elect a dissenting principle. The sole purpose of this person is to question every decision and even vote against it, even if they agree with it personally. In order to make sure there's no 'Yes Men' scenario and that you haven't formed, at worst case, an echo chamber.

TIP 4. DON'T WALK INTO A SITUATION YOU DON'T KNOW YOU CAN WALK OUT OF

Sadly, it's not unheard of that projects start without a plan B, or failed to launch plan, in place. This often occurs when a Risk Review hasn't taken place or, if it has, was done poorly. In business I've learned that for every success story there's a thousand more cautionary tales.

TIP 5. CONVENIENCE CAN TRAIN BEHAVIOUR

It can be very beneficial to leave educational material in common areas, most of the time people will learn passively. You can increase staff awareness and technical skills simply by leaving how-to books and security training material in lunchrooms, waiting rooms and other common areas. We've all read shampoo labels in the same place, and for the same reason.

TIP 6. TAKE SUGGESTIONS AND TIP-OFFS

Have a dedicated email solely for IT Security Suggestions and Tip-Offs. Having a dedicated email specifically for IT security suggestions and tip-offs can be extremely beneficial. It provides a direct and secure channel for employees to report potential security threats, share insights, and suggest improvements. This proactive approach helps in early detection of vulnerabilities and encourages a culture of security awareness within the organisation, ultimately strengthening the overall security posture.

TIP 7. ATTITUDE IS BIG

Attitude plays a crucial role in Cyber Security because it drives vigilance, proactivity, and resilience. A positive, proactive attitude ensures continuous learning and adaptation to evolving threats. A poor attitude is a poor security posture.

TIP 8. PERSONAL IT SECURITY IS A VITAL COMPONENT OF ORGANISATIONAL SECURITY HYGIENE

Each employee's commitment to their own personal IT security reduces vulnerabilities and prevents breaches, ensuring a more secure and resilient organisational environment. This collective effort strengthens the overall security posture. If an individual has personally become a victim of an IT cyber-attack, there is a chance your organisation is also at risk.

TIP 9. KANBAN

Yes, Kanban. Kanban is exceptionally helpful in Cyber Security and project management due to its visual workflow representation and flexibility. By visualising tasks on a Kanban board, teams can easily track progress, identify bottlenecks, and prioritise critical security tasks. This approach ensures transparency, enhances collaboration, and facilitates continuous improvement.

TIP 10. DEDICATE A TIME FOR REFLECTION

Dedicating time for reflection is crucial for effective cyber posturing. Regular reflection periods allow teams to review security practices, assess the effectiveness of current defences, and identify areas for improvement. This proactive approach fosters a culture of continuous learning and adaptation, helping organisations stay ahead of evolving cyber threats. By analysing past incidents and successes, teams can refine strategies, enhance response protocols, and ensure a robust and resilient security posture.