Incident Response - Use CRM principles

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-11-29

Introduction

Dealing with large or complex incidents? You need to think about CRM (Crew Resource Management.

The concept of CRM originated in the Aviation industry when people realised that human error was playing an important part in planes basically falling out of the sky. Basically, people realised that humans don't cope with excessive information during stressful situations very well.

While **cybersecurity** is (mostly) not as life-and-death as plane crashes, during incidents we are faced with similar problems.

- We are often overwhelmed with information and have no easy way to determine what is relevant and what isn't. If you don't believe me here, look at your Slack or Teams channel for the last incident you worked on.

- We have to make snap decisions based on incomplete data.

- We are working towards the same goal as other people but end up pulling in different directions.

- While mistakes are not normally life-threatening, they can have significant financial impacts (and possibly career impacts).

CRM Principles

Taken together, this highlights that **Incident Response** is an ideal place to use the CRM principles. There are lots of approaches here but the "key" principles are:

- **Communication**. Everyone in the team has to communicate EFFECTIVELY. This is not about dropping a random comment in a Teams chat, or throwing half-completed ideas into the group. It is about understanding the message you want to send, sending it in a format the recipients can understand and process and then actively listening for any responses. People think this is easy, but it is probably the one thing we fail at the most.

- **Situational Awareness**. Understand the big picture. We get tunnel vision where the $THING we are working on is the most important thing ever, but we need to constantly assess where we are in the overall incident and what our colleagues are doing. This requires constant effort and attention. As you can guess, good Communication improves Situational Awareness.

- **Decision Making**. You won't always have all the information you need so be prepared to make decisions that might be wrong. If you've done the first two steps well, your

decisions will be as good as they can be. Make decisions but be open to new ideas/ information.

- **Problem Solving**. This is the most basic part of any incident. By definition, there is a problem. Avoid being fixated on doing things a certain way. Solve the problem you are faced with, don't be put off or upset because you can't use the tool or technique you want to use.

- **Flexibility**. This caps off the previous ones. Be flexible enough to adapt to the situation you are in. Have ideas and make decisions but understand that if your knowledge changes, your decisions can change. It is often hard to accept but the most important part of leadership is this flexibility. Refusing to change your mind when you get new data can be a catastrophic mistake.

Implementing CRM

While this is really (really) simple to write down, it can be harder to put into practice.

Step 1. You have to start somewhere. Spend a bit of time looking at your playbooks, processes and working practices. At each step check if it aligns to at least one of the principles above. If not make changes.

Step 2. You need to make this a way of working. Having policies isn't enough, it needs to be turned into a habit. Everything your DFIR teams do, from tabletops to threat hunting, to full intrusion response should adhere to the principles. It may be awkward initially but with a bit of practice, it gets better. Some ideas include:

- Have a scheduled break where everyone in the team spends a minute or two describing their understanding of the incident. This is good because it forces people to think about what others are working on.
- Run questions to and from the team. Ask them questions to check they know what other people are doing and give them the chance to ask questions about the ongoing situation.
- Verbalise decisions, assumptions and limitations. When decisions are made, explain the assumptions and knowledge gaps that led to the decision. Frequently restate assumptions to check they are still valid. Encourage everyone to be open about what they don't know. Avoid the TV trope of "we dont have time to explain", time spent explaining saves time later on.

Step 3. Drive improvement. Get feedback. Identify what has worked well and what hasn't. Make the necessary changes to drive improvement. Be careful at the start though, as any change is likely to get some resistance simply because people dont like change. This isn't saying CRM has to be forced on everyone no matter if it works or not, instead just be careful that the feedback is valid, honest and relevant, rather than just sour grapes.

Want to learn more?

Interested in applying CRM to CyberSecurity incident response? Consider the SANS Institute's FOR608 course, "Enterprise Class Incident Response and Threat Hunting." This six-day course combines soft skills and technical knowledge needed by good incident responders to help them scale up to dealing with multiple intrusions on incredibly large networks.

You can find out more about the course at https://sans.org/for608.

Also, have a look at the SANS Digital Forensics and Incident Response page for the latest news on world-class DFIR training.

Further reading

1. Aviation Professional (n.d.), "Crew Resource Management (CRM)", *Aviation Professional*, available at: www.aviation-professional.net. This source explains that CRM, originally called Cockpit Resource Management, emerged after recognising that the technical skills of piloting were insufficient to ensure safety. It was found that accidents were often due to reasons other than inadequate piloting skills, leading to the development of CRM to optimise the use of all available resources by aircrew for safe and efficient flight operations.
2. Lauber, J.K. (1984), "Resource management on the flight deck", *Proceedings of a NASA/Industry Workshop*, NASA Conference Publication 2315, NASA-Ames Research Center, Moffett Field, California. This source is referenced in the Aviation Professional article as defining CRM in aviation as the optimal use of all available resources by an aircrew for safe and efficient flight operations.
3. Ruffel-Smith, H.P. (1979), "A simulator study of the interaction of pilot workload with errors, vigilance, and decisions", NASA TM-78482, NASA-Ames Research Center, Moffett Field, California. Ruffel-Smith's research analysed crew behaviour in flight simulators, showing that better resource use and communication within the crew led to improved performance.
4. United States National Transportation Safety Board (NTSB) (1979), "Aircraft Accident Report - United Airlines, Inc., McDonnell-Douglas DC-8-61, N8082U, Portland, Oregon, December 28, 1978", *NTSB Report Number AAR-79-7*. This report highlights a significant CRM-related accident where a failure in non-technical skills, particularly in crew communication and decision-making, was a contributory factor. Following this, NTSB issued a landmark recommendation to require CRM training for airline crews.

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858