



## Case Study

How CISOs can avoid being  
caught with their pants down



### A look at Australia's Victorian State Emergency Services cyber security training

James Fell is the CISO for the Victorian State emergency services under the department of the Premier and Cabinet. He's in charge of cyber security for Victoria's 8 critical infrastructure entities under Emergency Services.



© Copyright 2022 CybergymIEC



## The Reality: SOC teams are not trained for Incident Response (IR)

**The sooner CISOs accept that their SOC is likely not prepared to respond to an actual event, the sooner they can fix it.**

As a CISO in charge of 8 critical infrastructure entities, James Fell wanted to assess his teams to find out everybody's skills. At first glance, some of the agencies seemed to be in a decent position around detection and incident response. But then he dug a bit deeper through individual conversations...

Many were woefully unprepared for an actual IR, even though they had done an IR exercise at some point. The "exercise" consisted of a table top IR exercise or simply reading a document.

“

*There's no way you can expect your staff to perform in any good capacity if you've never given them proper training for a real cyber incident.*

CIO

”



# The Challenge: Moving from preventing to responding to an actual incident

**Solutions are deployed to detect.  
But what if an attacker gets through?**

We're trained to deploy and maintain new solutions that detect threats, but we're not trained in how to use the solution in the event of an IR. We need to get a firm grasp of the technical nature of how to do IR.

## Enter CybergymIEC's training

- Incident Response Principle Tactics Training
- SOC Intrusion Detection Training
- Advanced Forensics Collection Training
- Memory Forensic Techniques Training

By seeing and experiencing actual attacks on the screen, we were able to technically identify and label suspicious signs as an IOC (indicator of compromise) or an unknown IP. This enabled us to begin to know how to respond, to attempt to block it. We were also able to gain insights on what the hacker was doing and predict his end goal.



//

Wow. So that's what it's like.

**3 CISOs in the training**

//



# The Solution: Role-based training

**We determined each person’s current skill level and what they needed to know depending on their role**

We started training by agency but quickly realized that the individuals’ knowledge, skill levels and capabilities were too diverse. We switched to grouping the training into roles. Then we assessed each person’s skills and determined what they needed to learn to properly handle an actual IR.

//

*Table top exercises are still important, but we must train our staff to deal with the technical components of an IR.*

**James Fell, CISO Victoria State Government**

//




# The Result: The CISOs’ eyes were opened

**After the training, they wanted more!**

By creating role-based training, we were really able to meet everybody where they were according to their knowledge, skill levels and capabilities. Then we gave them the training they needed to capably handle an actual IR.

Now at CybergymIEC, we are developing role-based training programs for other critical infrastructure sectors.

//



*Everyone knows it’s going to happen, so you just have to train your staff to know how to deal with it technically.*

**James Fell**

//

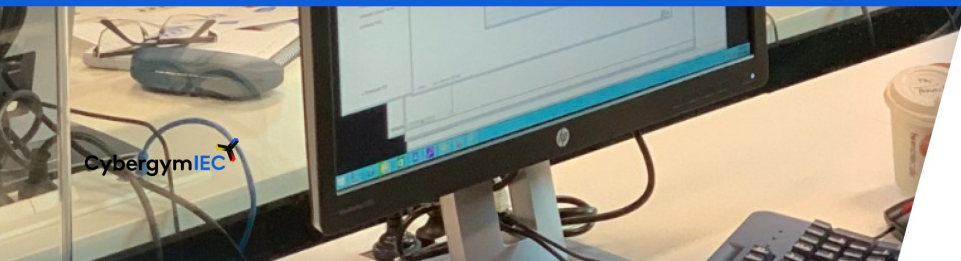


//

*"Compliance is not the outcome. It's awareness, performance, and governance."*

Mike Cohen, Sr. Account Director, CybergymIEC

//



## Conclusion

We can continue misbelieving our SOC teams are ready and qualified to handle an IR, but with no real training available until now, how can they be qualified? If an attack gets through your defenses, and the SOC is not ready, the responsibility falls on their leader.

Would you like to hear what training for your staff would look like? Contact us:

[cybergymiec.com](https://cybergymiec.com) | [sales@cybergym.com](mailto:sales@cybergym.com)

