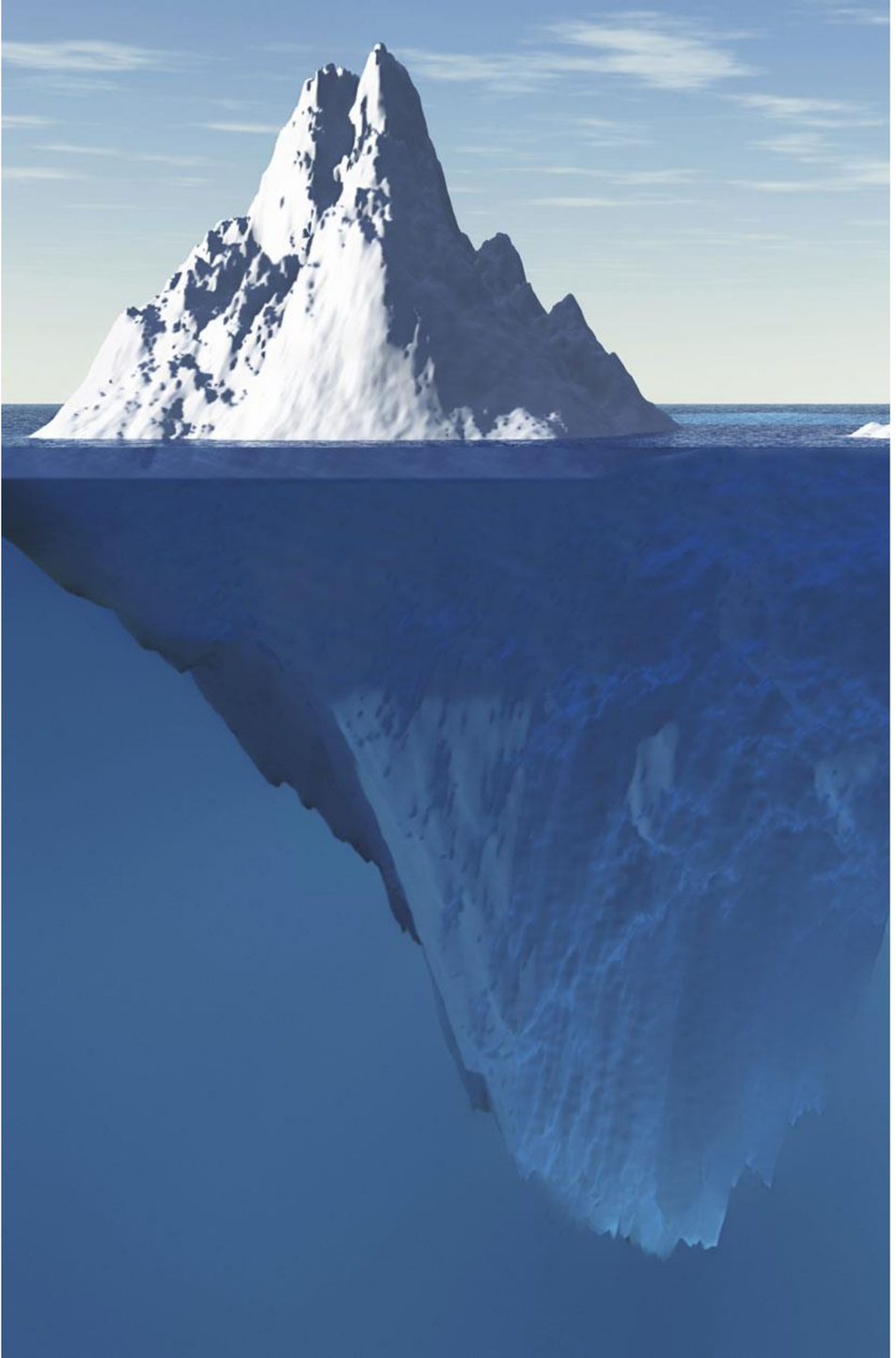
ARE YOU READY FOR WHAT IS COMING OVER THE HORIZON

Presented by:

BULLETPROOF

a GLI company



IT'S WHAT YOU DON'T KNOW THAT MAKES YOU **VULNERABLE**

- Cyber Attack Landscape
- What Happens After a Breach?

Gambling on security?

The average mean time to detect an incident in organizations is over *140* days.

How much damage could some hacker do to your data or more importantly your reputation if they had that much time?

SOC services are about reducing that number.

1 EXAMPLE
BAD RABBIT

REAL WORLD TURBULENT TIMES

2 Billion records compromised in the last year

8350 % increase in Ransomware usage

197+ DAYS between breach and detection

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

WHAT HAPPENS WHEN YOU'VE BEEN **BREACHED**?

1 INCIDENT QUALIFICATION	2 DETERMINE SCOPE OF BREACH	3 TRIAGE	4 RECOVERY AND/OR MITIGATION
5 DATA COLLECTION	6 FORENSICS	7 COMMUNICATIONS CO-ORDINATION	8 POST MORTEM

Sounds like a lot of work with masses of data?!

REACTIVE MANAGEMENT

BEST PRACTICES – FORENSICS

- **IDENTIFICATION AND/OR NOTIFICATION**
- **ISOLATION AND CAPTURE**
- **SCOPE MANAGEMENT**
- **FORENSIC DEEP DIVE**
- **RESOLUTION AND VERIFICATION**
- **RISK MANAGEMENT FOLLOW-UP**

Incident Response Team

Tools & Processes

Communication Strategy

WHERE DO WE STAND

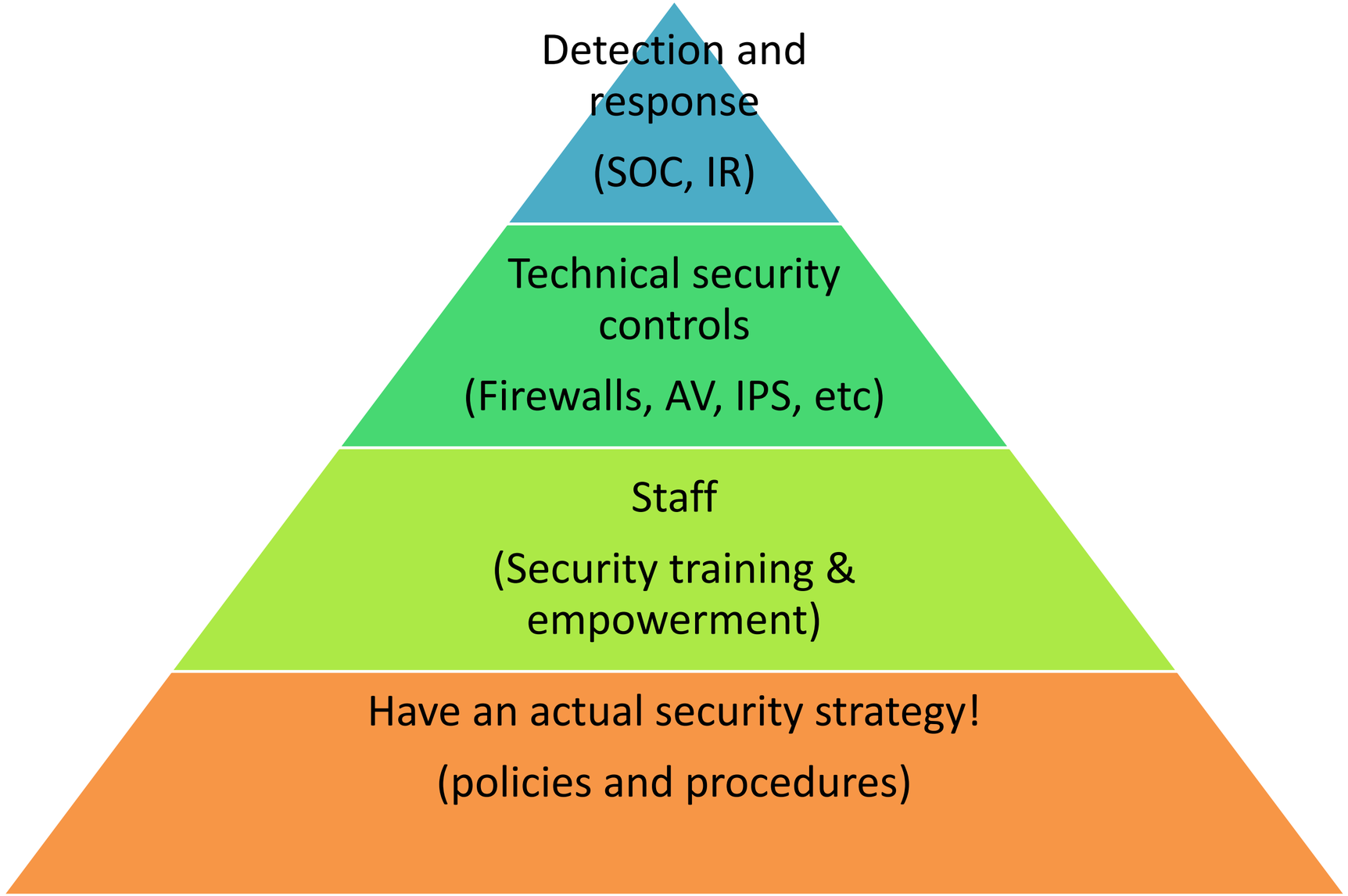
Public Safety Department says Canada successfully blocks some 600 million attempts each day to identify or exploit vulnerabilities in its government computer networks. http://ow.ly/kjt630gjbEe

BEST DEFENCE – PROACTIVE MANAGEMENT

Full Lifecycle Security Management

- Data analytics and trend analysis
- Log collection and correlation
- Security Information and Event Management (SIEM)
- Producing and responding to alerts
- Security incident confirmation
- Triage
- Incident response
- Communications and team coordination

Where does a SOC fit in your security strategy?



STAY DILIGENT