Incident Handling

Overview

- Introduction
- Incident Response Cycle [1]
- Conclusions

Reference:

1. CREST Cyber Security Incident Response Guide

Introduction

INCIDENCES – ATTACKS - CHALLENGES

Definition

"The UK Government Communications Headquarters (GCHQ) now sees real and credible threats to organisations through cyber security attacks on an unprecedented scale, diversity and complexity. We've seen determined and successful efforts to:

- *Steal intellectual property;*
- *Take commercially sensitive data, such as key negotiating positions;*
- *Gain unauthorised access to government and defence related* information;
- *Disrupt government and industry service; and, exploit information security weaknesses through the targeting of partners,* subsidiaries and supply chains at home and abroad.

The magnitude and tempo of these attacks, basic or sophisticated, on UK and global networks pose a real threat to the UK's economic security. The mitigation of these risks and management of these threats - in other words, cyber security - is one of the biggest challenges we all face today."

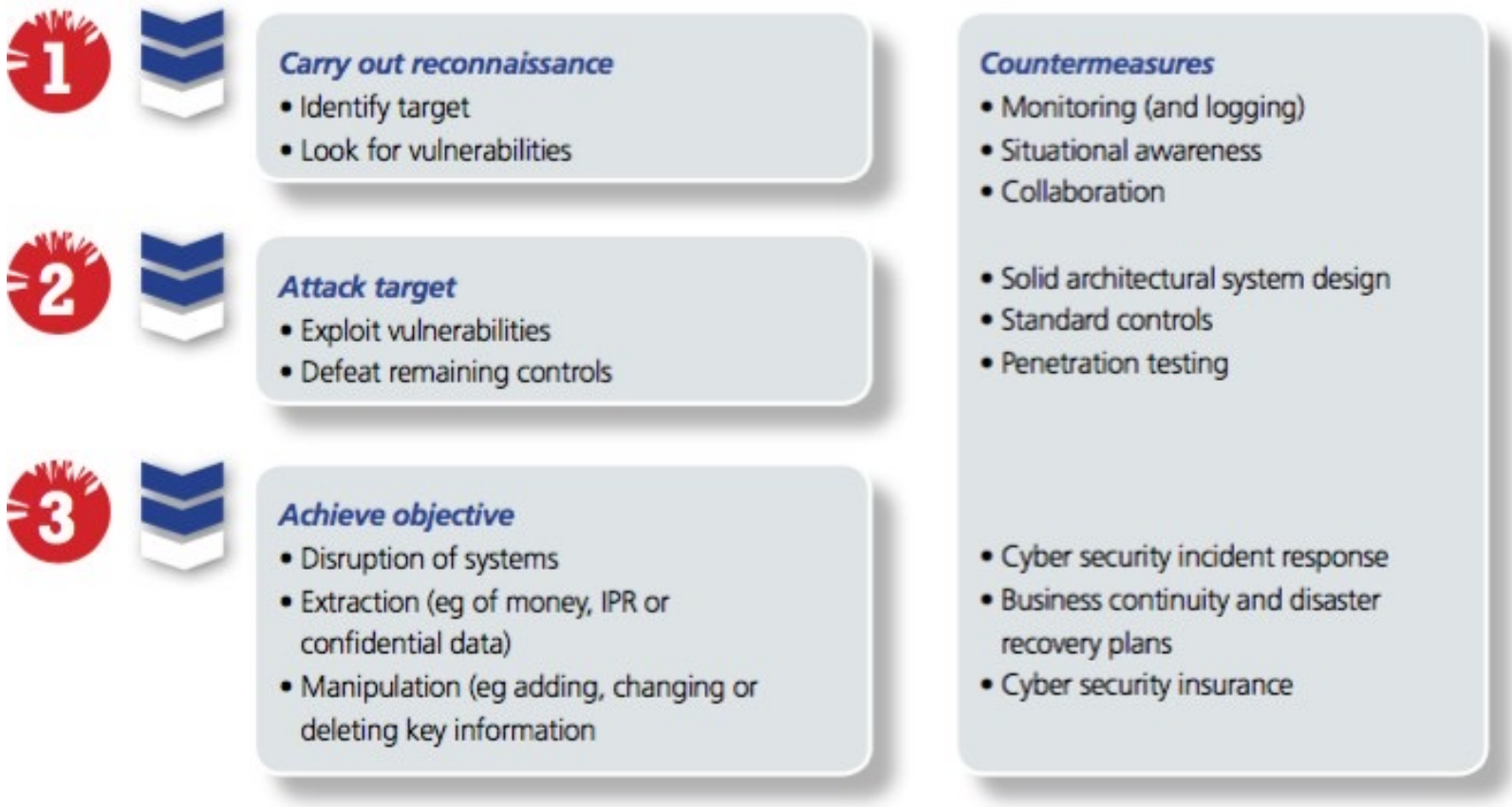
Source: 10 Steps to Cyber Security

Cyber Security Incidents



Source: CREST Cyber Security Incident Response Guide

Typical phases of a cyber security attack



Source: CREST Cyber Security Incident Response Guide

Advanced Persistent Threats

- Persistent threats by organised crime, military, commercial, and state-sponsored groups
- Often involve
  - Intelligence gathering
  - Initial exploitation
  - Command and control to achieve persistent access
  - Privilege escalation
  - Data exfiltration
- Many APTs can circumvent traditional security controls

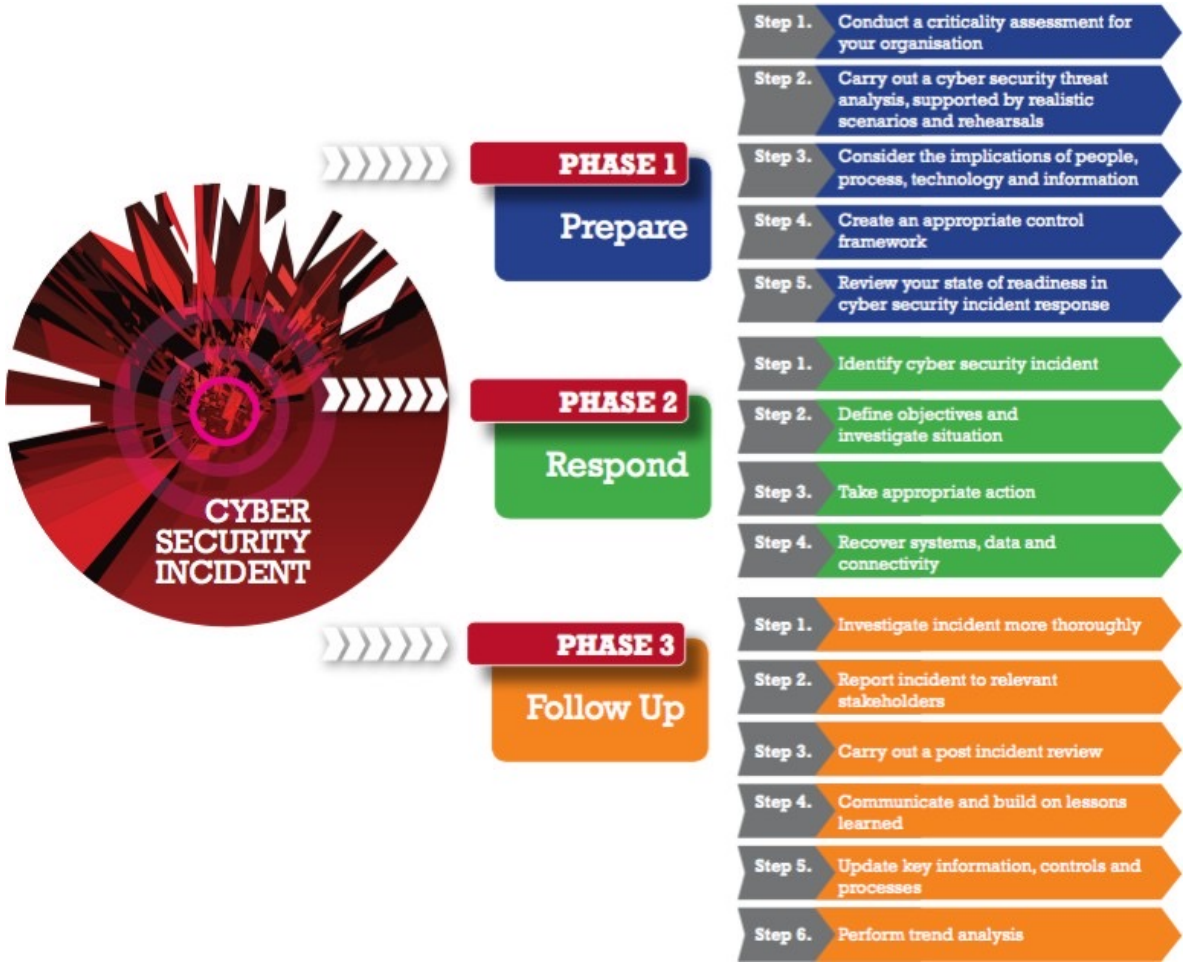
Main challenges in Cyber Incident Response

1. Identify suspected incident
2. Establish objectives of investigation and response
3. Analyse available information
4. Determine what actually happened
   DDoS, malware, system hack, session hijack, data corruption, etc
5. Identify what internal assets have been compromised
6. Determine what information has been disclosed/deleted/corrupted
7. Find out who did it and why
8. Work out how attacker got initial entry
9. Determine potential impact
10. Conduct sufficient investigation to identify and prosecute perpetrators

Incident Response Lifecycle

PREPARE – RESPOND – FOLLOW UP

Cyber Incident Response Cycle



Source: CREST Cyber Security Incident Response Guide

Activity

Open Cyber Security Incident Response Guide
Read section Phase 1 – Prepare
Menti

Phase 1 - Prepare

1. Conduct criticality assessment
   - Define critical assets, threats
   - Apply relevant security controls
   - Raise awareness on the need for effective cyber security response
   - Determine likely business impact of possible incidents
2. Carry out cyber security incident threat analysis
   - Technical infrastructure supporting critical assets
   - Cyber security threat landscape
   - Threats you are concerned about
   - Sources of threats
   - Possible threat vectors for attacks to exploit (eg internet, unauthorised USB sticks, etc)
   - Vulnerabilities to each threat

Phase 1 - Prepare

3. Consider implications on
   - People
     organise formal cyber incident response team
   - Process
     determine methodologies for dealing with incidents
   - Technology
     configure systems/networks/controls to aid detection and response
   - Information
     establish relevant information readily available (network map, IT infrastructure, key suppliers, business management, etc)

Phase 1 - Prepare

4. Create appropriate control environment[1]
   - Patch management policy, access control, firewalls, content inspection, backup
   - Multi factor authentication, Digital certificates, whitelisting, IDS, IPS, DLP (data loss prevention)
   - Continuous monitoring, Proactive APT assessments, System virtualisation, Sensitive network/data segregation, counterintelligence operations
5. Review state of readiness
   - Determine level of maturity
   - Organisations with mature incident response capability may conduct operations in-house; less mature may want to outsource

[1] 10 Steps to Cyber Security: http://www.gchq.gov.uk/Press/Pages/10-Steps-to-Cyber-Security.aspx

Phase 2 - Respond

1. Identify Cyber Security Incident
   - Identify suspected incident
   - Analyse available information
   - Determine what actually happened
   - Determine if this is organised cyber security attack or not
2. Define objectives and investigate situation
   - Understand the incident
   - Use Cyber Threat Intelligence (CERT-Computer Emergency Response Team, government, third parties)
   - Conducting triage (classify, prioritise, assign to personnel)
   - Carrying our first response

Phase 2 - Respond

Precursor: sign of incident to come
Indicator – sign of incident that may have occurred

Examples of possible cyber security incidents	The sources of these signs include.....
Precursors can include: • Web server log entries that show the usage of a vulnerability scanner • An announcement of a new exploit that targets a vulnerability of the organisation's mail server • A threat from a group stating that the group will attack the organisation. Indicators (there are many) can include: • A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server • Antivirus software alerts when it detects that a host is infected with malware. • A system administrator sees a filename with unusual characters • A host records an auditing configuration change in its log • An application logs multiple failed login attempts from an unfamiliar remote system • An email administrator sees a large number of bounced emails with suspicious content • A network administrator notices an unusual deviation from typical network traffic flows.	• Security software (eg IDS, IPS, DLP, SIEM, antivirus and spam software, file integrity checking software, monitoring services (often provided by a third party) • Logs (eg operating system logs, service and application logs, network device logs and network flows) • Publicly available information (eg information on new exploits, information exchange groups, third party organisations, governments) • People form within your organisation • Third parties (eg customers, suppliers, IT providers, ISPs, partners; government bodies).

Phase 2 - Respond

3. Take appropriate action
   - Contain incident
   - Eradicate the cause of the incident
   - Gather and preserve evidence
4. Recover systems, data and connectivity
   - Confirm remediation has been successful
   - Recovery plans should include
     - Rebuild infected systems
     - Replace compromised files with clean versions
     - Remove temporary constraints during containment period
     - Reset passwords on compromised accounts
     - Install patches, change passwords, tighten n/w perimeter
     - Test systems thoroughly

Phase 3 – Follow up

Following up a cyber security incident

1. Investigate incident more thoroughly
2. Report to relevant stakeholders
3. Carry out post-incident review
4. Communicate and build on lessons learnt
5. Update key information, controls and processes
6. Perform trend analysis

Phase 3 – Follow up

1. Investigate incident more thoroughly
   - Problem cause analysis, root cause analysis, quantify business impact
   - Identify perpetrator?? (often involves forensic analysis)
2. Report to relevant stakeholders
   - What do I have to report?
   - Who to report to (Law enforcement, CERTs, regulatory bodies, partners, etc)?
   - How much should I share?
   - In what format do I report?
3. Carry out post-incident review
   - How well did staff handled incident?
   - Was information available?
   - Were there unforeseen events that could have been prevented?
   - What corrective actions could prevent similar incidents in future?
   - What lessons have been learnt?

Phase 3 – Follow up

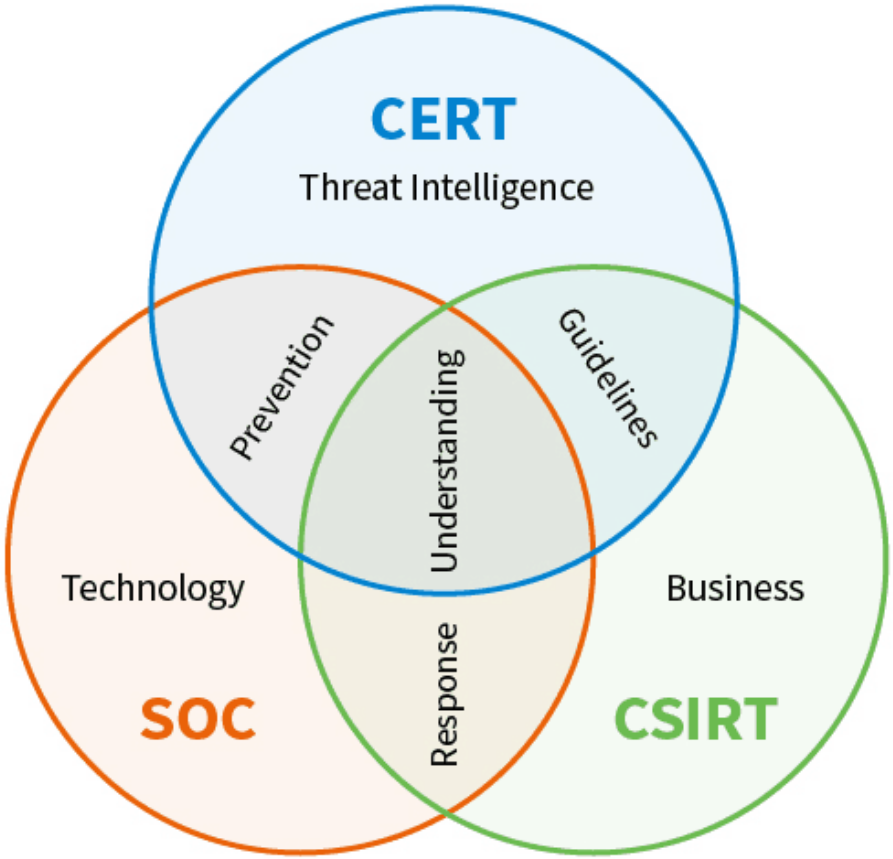
4. Communicate and build on lessons learnt

5. Update key information, controls and processes

6. Perform trend analysis
   - Evaluate patterns and trends of incidents
   - Identify common factors that have influenced incidents
   - Determine effectiveness of controls
   - Understand costs and impacts

Roles

Security staff working in a security operations centre are often called the SOC team



CERT: computer emergency response team

CSIRT: Computer Security Incident Response Team

SOC: security operation center

Roles

Primary Objective	Organization Type	Rationale
Collect and Disseminate Security Information	CERT	A CERT is equipped to collect and curate security information from several sources but not to defend a network or respond to individual incidents.
Monitor and Defend an Organization's Infrastructure	SOC	A SOC is an organization that invests in technology and staff skilled at monitoring and defending networks, endpoints, servers, and other infrastructure.
Respond to Security Incidents	CSIRT	A CSIRT is a cross-functional organization that is chartered with responding to security incidents. Some team members may not be full time but are called in as needed.

Monitoring & Defending Roles

If your team roles include monitoring and defending an organization against cyber attacks, you are building and staffing a SOC. A small company may not be able to afford a SOC, then you will want a CSIRT to deal with security incidents as they occur.

Common staff roles:

Team Leader or Executive Sponsor: CISO (Chief information security officers) or executive staff that communicates incidents to the executive staff / board and to assure that the CSIRT gets appropriate attention and budget.

Incident Manager: works across the organization and is responsible for calling meetings and holding team members accountable for action items. Summarizes and communicates findings and impacts throughout the company and escalates major issues up to higher levels.

Monitoring & Defending Roles

Lead Investigator: A technical resource, security analyst or dedicated incident responder, investigates security incidents. They may work with an extended team of security analysts and forensic investigators.

Investigators: A technical resource that normally works in a team, some teams ask for technical specialties

- **Communication skills.** Whether in emergency mode, or effectively with clients, the public and executives. Written communication is also important, as members need to be able to write effective policies, documents etc.
- **Listening skills.** Concerns and requests of clients as well as management.
- **Tact and diplomacy.** Emergencies with anxious, angry customers and/or managers.
- **Teamwork.** Intricate professional groups with different skills, experience and roles.
- **Trustworthiness and discretion.** Access to sensitive data and vulnerabilities.
- **Problem solving.** Not all incidents are created equal, unexpected situations happen.
- **Ability to cope with stress.** (more on this in a bit)
- **Organizational skills.** Organize the work, prioritize it and apply time management.

Monitoring & Defending Roles

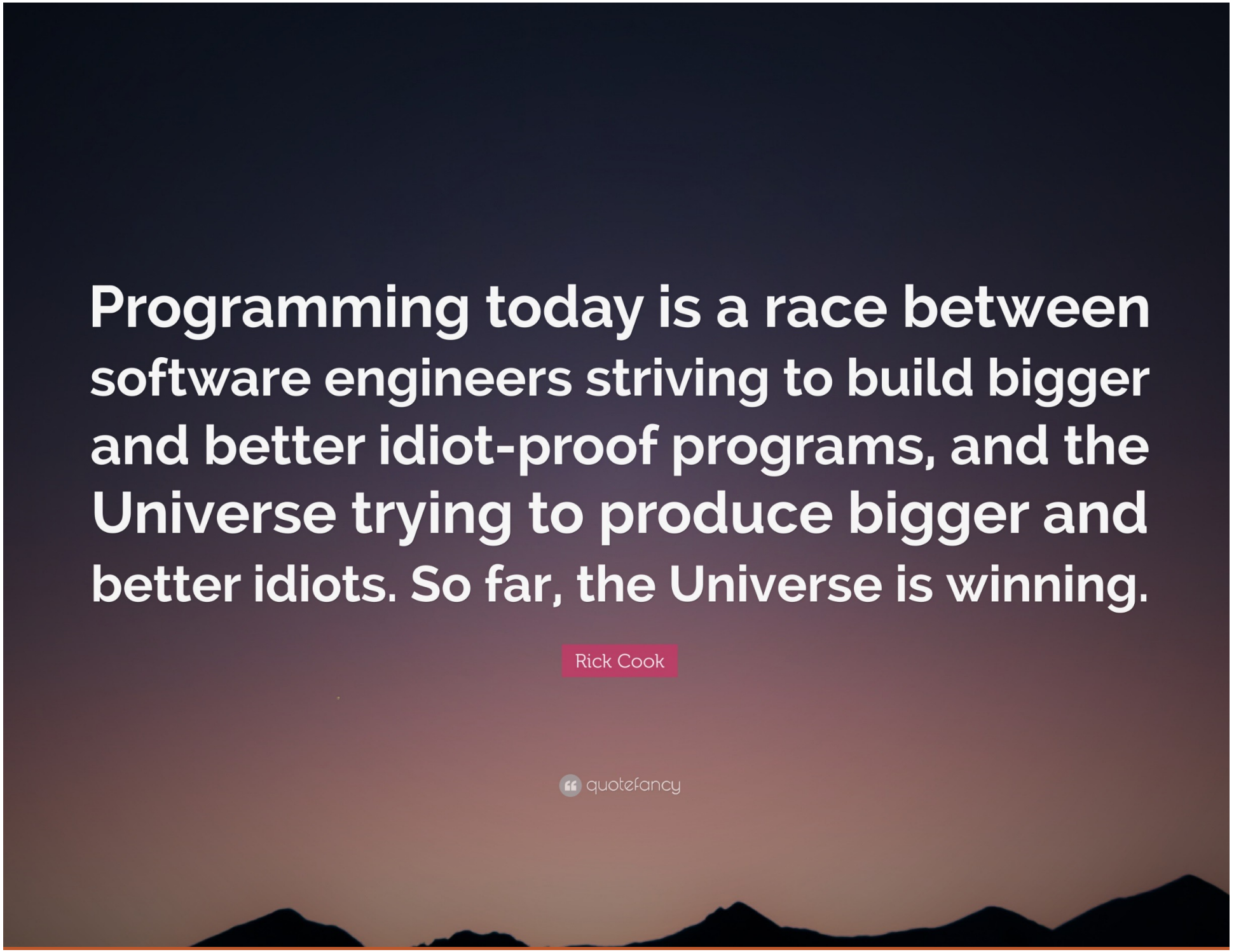
Communication and Public Relations: Might be on marketing team, responsible for public relations, fielding any press inquiries or statements, as needed, and drafting communications to be sent to employees, partners, and customers.

Legal: General council / deputy member of the legal team, advises on the need to disclose incidents, such as a breach, and deals with any of the fallout resulting from security incidents, such as shareholder or employee lawsuits.

Human Resource Representative: This position is typically filled by the head of HR, who can manage any personnel-related issues that occur, especially if they involve insider theft. The HR representative also gives suggestions for how incidents are communicated to employees.

Outsourcing versus internal

CSIRT Functions to Consider Outsourcing	Pros	Cons
Incident Response Plan (IRP) Creation	There are consultants who are expert in IRP creation.	A plan created by a third party may not have internal ownership and oversight.
Monitoring	A managed security service provider (MSSP) or managed detection and response (MDR) vendor can be a fit for organizations that are not staffed 24/7 or lack expertise.	There may be a time lag between event detection and commencement of investigation. Also, outsourcing will not relieve your organization from legal responsibility.
Investigation	There are computer forensics firms that are experts in dealing with investigations.	It may take time to onboard an external forensics experts, and they are typically costly.
Remediation	You may find more security expertise in a third party.	External teams may not have the access rights and context to properly address the issue.
Internal Communications	There really is no positive advantage to using a third party.	This critical function should not be handled by a third party.
Public Relations	Your PR firm may be able to act quickly. There are also firms that specialize in crisis communications.	Your PR firm may not be as familiar with the business and risks in your market, and may also be dealing with sensitive information.
Legal	Your external counsel may have handled a similar incident for another client.	Typically, external counsel may be slower to react than internal counsel, who will need to be involved regardless.


Programming today is a race between software engineers striving to build bigger and better idiot-proof programs, and the Universe trying to produce bigger and better idiots. So far, the Universe is winning.
Rick Cook
quotefancy

The stress

Is Cybersecurity One of the Most Stressful Career Paths?

* the average job tenure of a CISO is just 18-24 months — much shorter than the average 8.4-year tenure of CEOs. Security professionals in particular are:

More than 2x as likely to report poor work-life balance (44 vs. 20 %)

More than 5x as likely to worry about job security (32 vs. 6 %)

More than 3x as likely not to take full vacation days (89 vs. 28 %)

https://securityintelligence.com/articles/9-reasons-why-cybersecurity-stress-is-an-industry-epidemic/

The Stress

1. Resource Shortages & Skills Shortages

2. Internal Pressures: Thirty-eight percent of cyber pros say they're frustrated with trying to educate end users to change their behaviors. Additionally, 18 percent of CISOs believe fellow board members are indifferent to security or view it as an inconvenience.

3. Overwhelming Workloads: 73 percent of security practitioners surveyed by the Ponemon Institute say an ever-increasing workload is causing burnout. SOC analysts are particularly likely to feel overwhelmed for many reasons, according to the same report. Sixty-five percent of SOC analysts have considered a job change because workload frustrations are compounded by poor visibility or alert fatigue.

The Stress

4. On-Call Requirements: 71 percent of security employees report they're on call 24/7/365, per Ponemon.

5. Work Hours: The overwhelming majority of cybersecurity pros (88 percent) admit they work more than 40 hours each week, per Nominet.

6. Securing Transformation: Securing new IT initiatives stresses 40 percent of cyber pros, according to ESG. Teams have to create security controls at the speed of innovation to address the risks of new cloud or internet of things (IoT) initiatives. In addition, shadow IT is a major struggle — 39 percent of security pros are irritated by unpredictable requirements to secure technology projects which are started without cyber's knowledge or input.

Conclusions

- Cyber security incidents, such as Advanced Persistent Threats are here to stay
- The type of cyber security incident depends on the source (minor criminal compared to major organised crime syndicate), rather than the type of incident
- It is difficult to identify the type of cyber security incident until further investigation has been carried out
- Cyber security incident response maturity varies considerably among organisations
- There are significant challenges in terms of preparing for, responding to and following up incidents
- Depending on level of maturity, organisations may need to outsource

Thank You