PESU Center for
Information Security,
Forensics and
Cyber Resilience

Welcome to

PES University

Ring Road Campus, Bengaluru

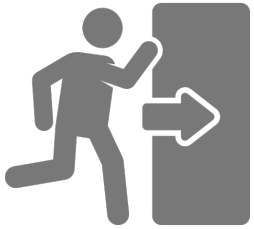
PESU Center for
Information Security,
Forensics and
Cyber Resilience

Computer Network Security

UE23CS343AB6

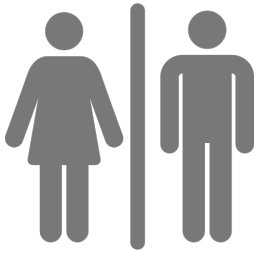
Prasad Honnavalli, Prof. Preet Kanwal, Dr. Gokul Kannan Sadasivam

Unit 4, Lecture #4



Emergency Exit

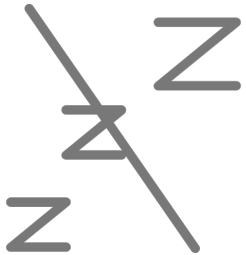
Assembly Point



Washroom

No Chatting

Phones on silent



No Sleeping

Disclaimer

- *This presentation is purely educational.*
- *The views expressed by the presenter is not representation of any organization.*
- *The views are based on professional experience of the presenter and no liability is accepted by the presenter in the event of any potential or perceived losses resulting from this presentation.*

A Note on Security

- In this course, you will be exposed to information about security problems and vulnerabilities with computing systems and networks.
- To be clear, you are not to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network without the express consent of the owner.
- In particular, you will comply with all my instructions when doing the labs.
  - My instructions are in consonance with applicable laws of India and PES University policies.
  - If in any doubt, please consult your professor!
- Any violation is at **YOUR RISK!**
  And may result in severe consequences.

Ethics Guide

- Of necessity, this class has a fair amount of "dark web" content
  - And a lot of "don't try this at home" stuff

- As defenders you must understand the offense:
  Big WORD is ***consent***
  - Its usually OK to break into ***your own stuff;*** its a great way to evaluate systems
  - Its usually OK to break into someone else's stuff ***with explicit permission to do so***
  - It is both grossly unethical and often ***exceedingly criminal*** to access systems ***without explicit permission or explicit authorization***

What is one word that comes to mind when you think of cybersecurity?

Your Personal Experience

- ☞ Experienced real time crisis?
- ☞ Victim of Cyber attack?
- ☞ Victim of Data Breach?

What will you learn?

- A cyberattack affects **Business Operations, Customer Trust, and Reputation**
- How to manage Cyberattack Crisis?
  - Breach of Data Security and Data privacy (Confidentiality, Integrity)
  - Business Continuity (Availability)
  - Disaster Recovery
  - Risk Management issues
- Importance of proactive practice to deal with Cyber Incidents
  - Incident response, tabletop exercises)
- How to build and improve Digital Resilience?
  - Visibility, Monitoring, NOT outsourcing Responsibility (Strong SLA)
- Importance of Periodic and effective Training of people
  - Effective communication, Leadership

*i*Premier Case

Network Security

Personalities

Name	Role at *i*Premier
Bob Turley	CIO
Joanne Ripley	Operation Team Leader
Jack Samuelson	CEO
Warren Spangler	VP Business Development
Tim Mandel	CTO and Co-founder
Peter Stewart	Legal Counsel
Leon	Ops Team

*i*Premier Case - A

- **What does it "feel like" to be in Bob Turley's shoes?**
  - *What is it like to be awakened the way Bob Turley is in the case?*
  - *What are his impressions and experiences in the first few minutes after the telephone rings?*

*i*Premier Case - A

- **Listing ways to avoid unhelpful human tendencies**
  - *What advice might you give for dealing with crisis situations like this one?*
  - *What principles or recommendations might we follow during a crisis to avoid some of the problems inherent in such situations?*

*i*Premier Case -A

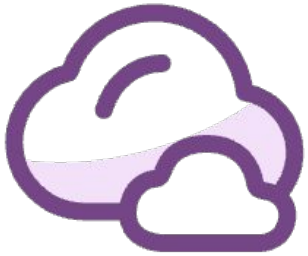
- *What are Bob Turley's and iPremier's priorities?*

*i*Premier Case - A

- *How did iPremier perform during the crisis?*
- *What might you have done differently during the crisis?*
- *How might they have been better prepared?*

*i*Premier Case - A

- *Disclosure – Analyst Meet*
  - *What information about these events should iPremier share with its customer and the public?*
  - *What is your strategy for the Analyst meeting?*
    - *What will you say?*
    - *What won't you say?*



What are some key challenges organizations face during a cyber crisis?

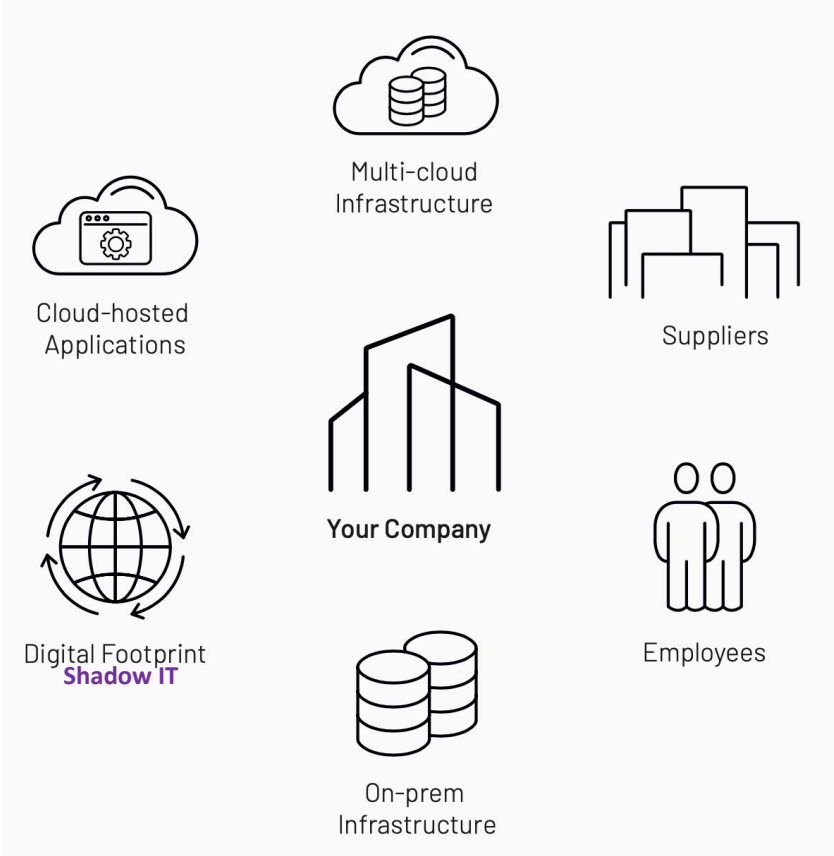
Could CIO be better prepared?

Unknown Attack surface –
are they advantageous to the adversary ?

The attack surface includes every potentially exploitable entry point that can be used by an adversary.

84% of security leaders worry they're missing threats and incidents because of alert and vulnerability fatigue

MANDIANT | GLOBAL PERSPECTIVES ON THREAT INTELLIGENCE



Example - IDS Alert

- During an investigation of a high-severity IDS alert, an analyst processed it according to the documented procedure.
  - It was a high-severity IDS event from a user's workstation to an internal web server.
  - However, the web server wasn't vulnerable to the attack, so the investigation was closed.
- The SOC manager did a review of high severity alerts later and recognized that the attack was launched from an internal asset against another internal asset.
  - This meant there was an attacker controlling a user's workstation.
  - The analyst had followed the written procedures for IDS events but failed in this case because the procedures were written with externally sourced attacks in mind.

Example – TLS Certificate

- During an investigation of what initially appeared to be commodity phishing and malware, analysis identified a specific TLS certificate within the payload uniquely used by FIN8 (https://attack.mitre.org/groups/G0061/).

- Based on this attribution, the incident responder targeted subsequent analysis to known persistence and privilege escalation techniques used by the adversary, which identified relevant forensic artifacts in mere minutes, compared to what would have otherwise taken hours or days to comprehensively review.

Example – VPN Compromised Credentials

- An adversary who used compromised credentials against the organization's VPN access was discovered.
- The organization detected account abuse when the adversary emailed the help desk asking for a password reset, the help desk responded, and the actual user reported the impersonation.
- With this alert, the initial evidence was limited to the IP address and the account used by the adversary.

CIO To-Do

Evaluate the data you rely on to ensure it is trustworthy, timely and actionable

A dependable threat intelligence program must be built on solid foundations; these attributes are an essential starting point.

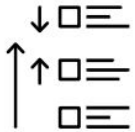
Understand active threats specific to your organization and industry

Build up a clear picture of the adversaries, their motives, and tactics, techniques and procedures (TTPs) to best adapt your defenses.

Communicate with your stakeholders

Develop a regular cadence of feeding relevant intelligence (tactical, operational or strategic) to the right stakeholder group to drive optimal security and business decisions all the way through to the senior leadership and board level.

CIO To-Do

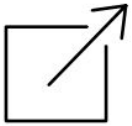


Prioritize resources to address what really matters

Leverage intelligence to understand what threats matter most to your organization right now. Assess vulnerabilities and exposures, give them a risk rating based on criticality and then tackle issues in the right order.

Test your defenses

Proactively test the organization's response to typical attack tactics from the adversaries you have identified. Validate your protection against these specific groups and measure improvements in your program over time.



Take action

Leverage the threat intelligence across your security systems and processes to proactively protect against potential threats.

Cybersecurity Frameworks

Applying Cybersecurity Frameworks to the *i*Premier Case

Cybersecurity frameworks formalize what good security and incident response look like..

☞ We examine the *i*Premier case through these frameworks:

- **CIS Controls (v8)** – tactical, technical safeguards
- **NIST Cybersecurity Framework (CSF 2.0)** – strategic, risk-based governance
- **NIST SP 800-61r2** – operational, step-by-step incident response lifecycle

☞ Each exposes specific gaps and highlights areas for improvement.

CIS Control 5 – Account Management

- **What it requires:**
  - Defined privilege levels
  - Properly documented admin accounts
  - Frequent privilege review
  - Clear ownership of credentials
- **iPremier gap:**
  - No one knew who had access to what on the Qdata infrastructure
  - CIO/CTO lacked admin control
  - Executives couldn't even log into systems to inspect logs
- **Takeaway:** Even outsourced systems require clear privilege governance and documented access control.

CIS Control 8 – Audit Log Management

- **What it requires:**
  - Logging of access, traffic, authentication events
  - Centralized log storage
  - Log integrity and retention
  - Regular log review
- **iPremier gap:**
  - iPremier had **no logs of its own**
  - Qdata controlled the monitoring and kept most logs
  - iPremier had no visibility into attack traffic
  - No alerting or anomaly detection
- **Takeaway:** Without logs, you cannot detect, investigate, or understand incidents.

CIS Control 13 – Network Monitoring & Defense

- **What it requires:**
  - IDS/IPS
  - Network traffic analytics
  - Real-time monitoring
  - Alerting on abnormal patterns
- **iPremier gap:**
  - No IDS
  - No bandwidth monitoring
  - No traffic dashboards
  - They depended entirely on Qdata's view of the attack
- **Takeaway:** Outsourcing hosting ≠ outsourcing responsibility for monitoring.

CIS Control 17 – Incident Response Management

- **What it requires:**
  - A documented incident response plan (IRP)
  - Defined roles and Clear escalation pathways
  - Routine tabletop exercises
  - Post-incident analysis
- **iPremier gap:**
  - No IR plan, No defined IR team
  - No communication plan
  - Zero post-incident review
- **Takeaway:** A cyber crisis is not the time to *improvise*. IR planning is essential for business continuity

NIST Cybersecurity Framework (CSF 2.0)

- *NIST CSF helps organizations manage cybersecurity risk at a strategic level.*
- *It has 5 functions:*
  - → *Identify*
  - → *Protect*
  - → *Detect*
  - → *Respond*
  - → *Recover.*

Identify

- **Expectation:**
  - Know assets, risks, dependencies, and organizational roles
  - Maintain inventory of systems and data
  - Understand business criticality
- **iPremier gaps:**
  - No inventory of systems hosted at Qdata
  - No understanding of data exposure risk
  - No clarity on who owns what during an incident
  - No defined cybersecurity governance structure
- **Takeaway:** You cannot protect what you do not catalogue.

Protect

☞ **Expectation:**

- Implement safeguards to reduce likelihood and impact of an attack
- Access controls, firewalls, DDoS protections, backups

☞ **iPremier gaps:**

- No DDoS protection or rate-limiting
- Poor network architecture visibility
- Lack of basic protective controls
- Over-reliance on ISP for protection

☞ **Takeaway:** Basic preventive controls (firewalls, rate limiting, redundancy) would reduce crisis severity.

Detect

- **Expectation:**
  - Identify abnormal behaviors
  - Monitor traffic, alerts, logs
  - Have dashboards and automated detection
- **iPremier gaps:**
  - No automated detection mechanisms
  - No logs → no signals
  - Entirely dependent on Qdata
- **Takeaway:** Detection is essential for early intervention and informed decision-making.

Respond

- **Expectation:**
  - Take coordinated action once an incident occurs
  - Defined roles, communication process, containment strategies
- **iPremier gaps:**
  - Confusion among executives (CEO vs CTO vs CIO)
  - No decision authority documented
  - Communication breakdown with Qdata
  - No predefined containment options (e.g., blackholing, throttling)
- **Takeaway:** Response must be pre-planned, rehearsed, and clearly assigned.

Recover

☞ **Expectation:**
- Restore services
- Communicate with stakeholders
- Perform post-incident review

☞ **iPremier gaps:**
- Unclear if customer data was exposed
- No PR or legal response
- No lessons-learned session
- No roadmap for preventing recurrence

☞ **Takeaway:** Recovery is both technical and reputational.
Post-incident reviews are mandatory for improving resilience.

NIST SP 800-61r2:

☞ *This* Computer Security Incident Handling *framework gives a real-world, step-by-step model for handling incidents.*

☞ It emphasizes four phases.

- Preparation
- Detection and Analysis
- Containment, Recovery
- Post Incident

Preparation

- **Expectation:**
  - IR plan
  - Roles defined
  - Tools (IDS, logging, scripts)
  - Training, tabletop exercises
- **iPremier situation:**
  - No IR policy
  - No assignments (CIO? CTO? CEO?)
  - No monitoring tools
  - No staff training, rehearsals
- **Takeaway:** Preparation is the most important phase — and iPremier was not prepared enough.

Detection & Analysis

- **Expectation:**
  - Detect attack quickly
  - Document timelines
  - Confirm scope and impact
- **iPremier situation:**
  - They didn’t know it was a DoS attack initially
  - No logs to analyze
  - Conflicting information from Qdata
  - Executive team completely in the dark
- **Takeaway:** Fast and accurate detection allows effective containment.

Containment & Recovery

- **Expectation:**
  - Take action to limit damage
  - Restore operations
  - Remove threat source
- **iPremier situation:**
  - No containment decisions possible
  - Unclear on whether to shut down the site
  - Reliance on ISP for entire recovery
  - No mitigation strategies available
- **Takeaway:** Containment and recovery require pre-planned options and authority to execute them.

Post-Incident Activity

- **Expectation:**
  - Review what happened
  - Identify root cause
  - Improve processes
  - Update policies
- **iPremier situation:**
  - No structured review
  - No documented lessons learned
  - No policy updates
  - Executive team wanted to “just move on”
- **Takeaway:** If you don’t learn from the incident, you could be a victim again!

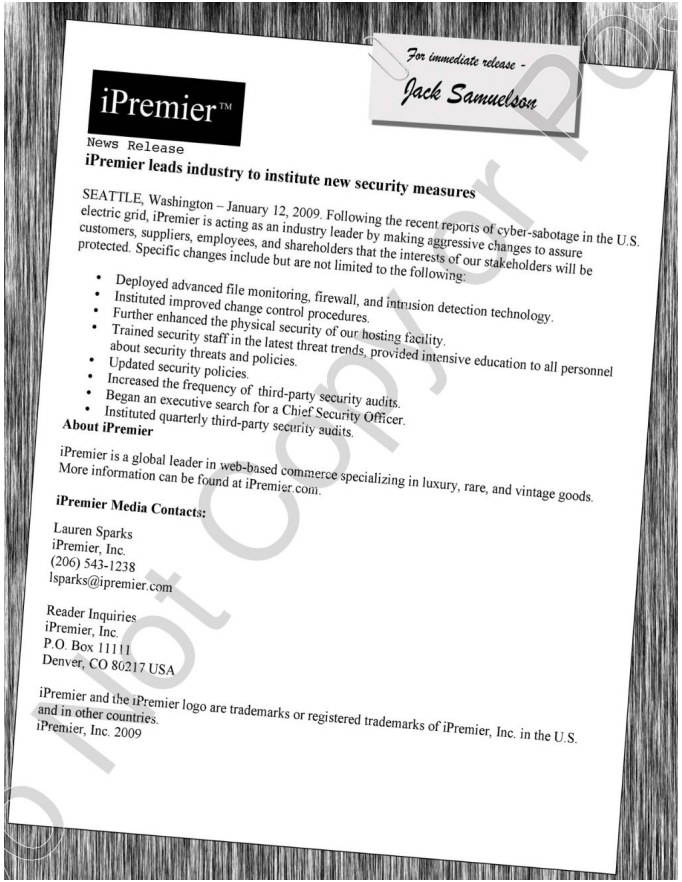
*i*Premier Case

Part B

*i*Premier Case – B

Exhibit 1 Security Measures Instituted by the iPremier Company Following January 2018 Attack

- Restarted all production computer equipment (not at the same time—no customer
- interruptions).
- Conducted a file-by-file examination of every file on every production computer to look for evidence of files or parts of files that should not be present.
- Began a study of technology solutions that might be used to assure that files on production computers were the same files initially installed there.
- Expedited a project aimed at moving to a more modern hosting facility.
- Modernized computing infrastructure to include a more sophisticated firewall.
- Bought additional disk space and enabled high levels of logging so there would be more diagnostic information available after any future attacks.
- Trained more staff in the use of monitoring software; educated all about security threats.
- Created an incident-response team and practiced a simulated attack.
- Began an executive search for a Chief Security Officer.
- Retained a cybersecurity consulting firm.
- Instituted monthly third-party security audits.



For immediate release -

Jack Samuelson

iPremier™

News Release

iPremier leads industry to institute new security measures

SEATTLE, Washington – January 12, 2009. Following the recent reports of cyber-sabotage in the U.S. electric grid, iPremier is acting as an industry leader by making aggressive changes to assure customers, suppliers, employees, and shareholders that the interests of our stakeholders will be protected. Specific changes include but are not limited to the following:

- Deployed advanced file monitoring, firewall, and intrusion detection technology.
- Instituted improved change control procedures.
- Further enhanced the physical security of our hosting facility.
- Trained security staff in the latest threat trends, provided intensive education to all personnel about security threats and policies.
- Updated security policies.
- Increased the frequency of third-party security audits.
- Began an executive search for a Chief Security Officer.
- Instituted quarterly third-party security audits.

About iPremier

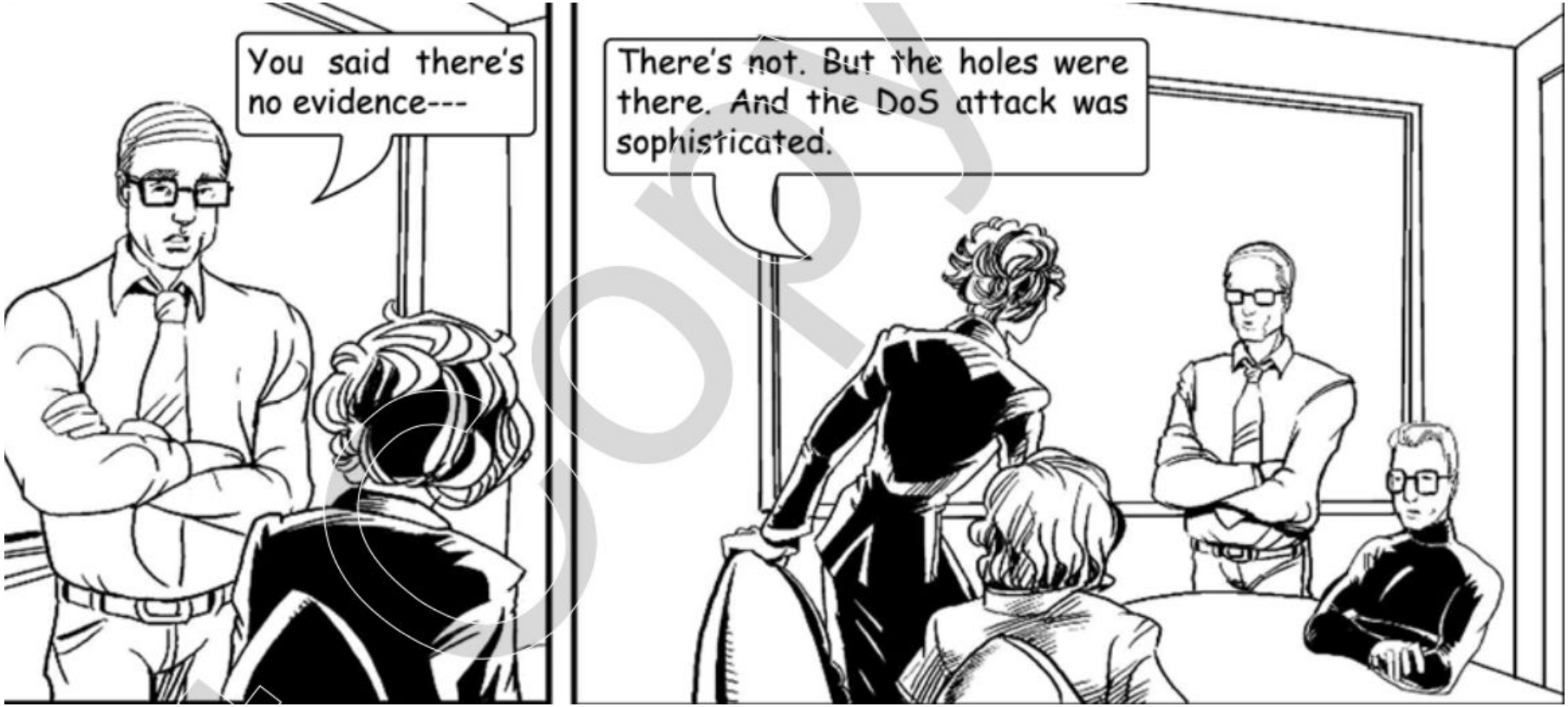
iPremier is a global leader in web-based commerce specializing in luxury, rare, and vintage goods. More information can be found at iPremier.com.

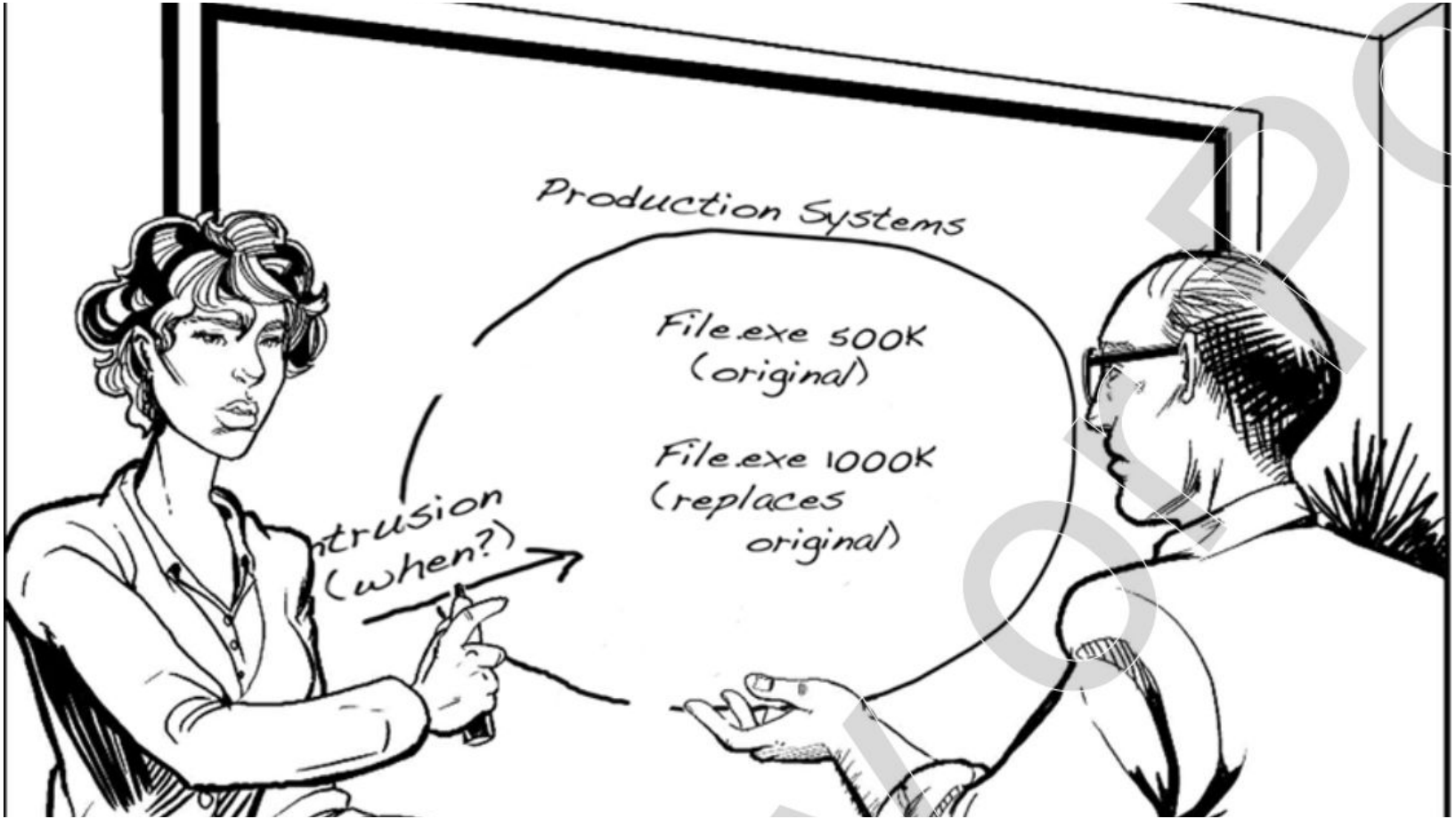
iPremier Media Contacts:

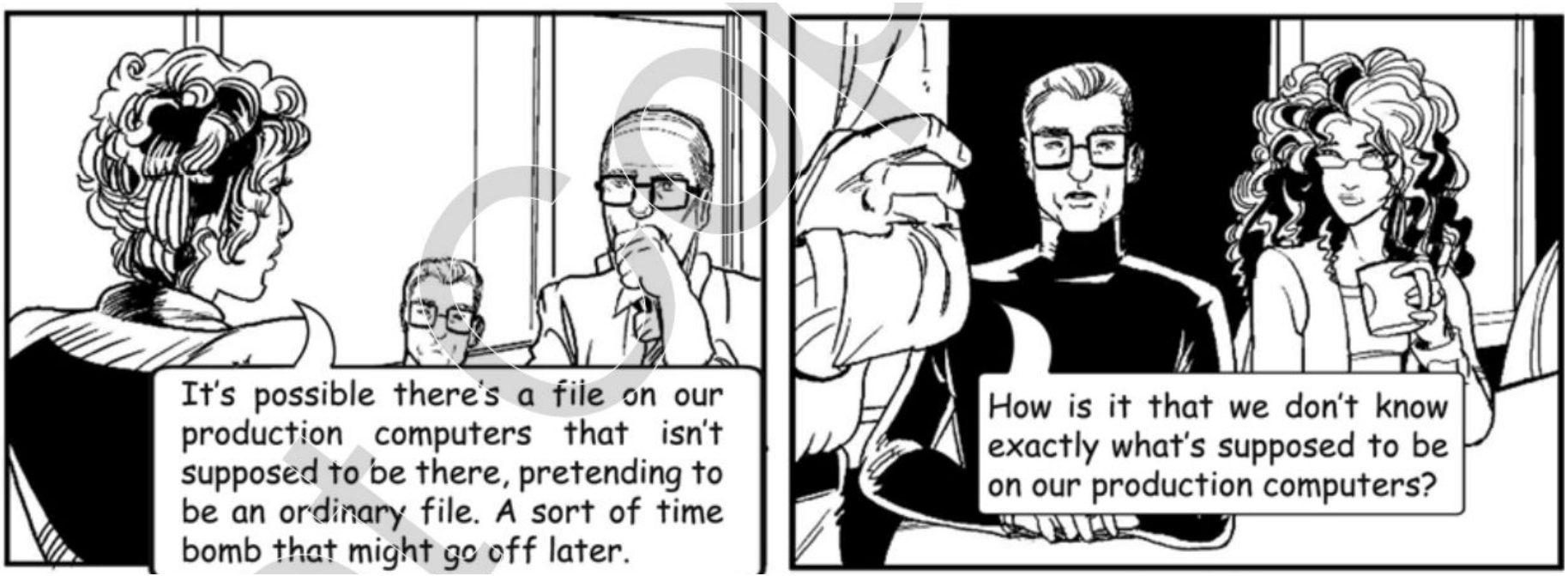
Lauren Sparks
iPremier, Inc.
(206) 543-1238
lsparks@ipremier.com

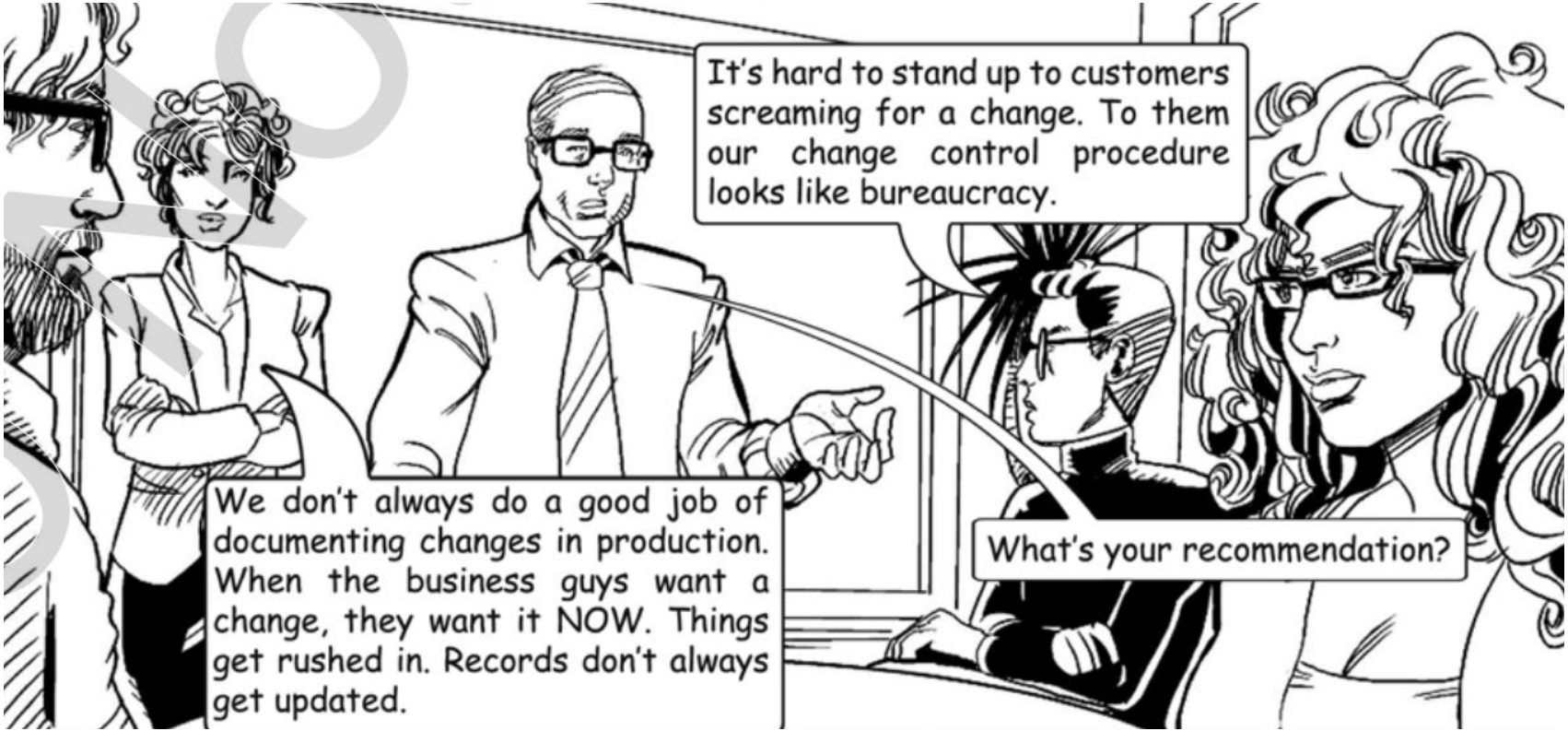
Reader Inquiries
iPremier, Inc.
P.O. Box 11111
Denver, CO 80217 USA


Our new security measures are supposed to close those holes. Am I missing something?
The bad guys could have already been inside, left something nasty behind.


You said there's no evidence---
There's not. But the holes were there. And the DoS attack was sophisticated.


Production Systems
File.exe 500K
(original)
File.exe 1000K
(replaces
original)
(when?)


It's possible there's a file on our production computers that isn't supposed to be there, pretending to be an ordinary file. A sort of time bomb that might go off later.
How is it that we don't know exactly what's supposed to be on our production computers?


It's hard to stand up to customers screaming for a change. To them our change control procedure looks like bureaucracy.
We don't always do a good job of documenting changes in production. When the business guys want a change, they want it NOW. Things get rushed in. Records don't always get updated.
What's your recommendation?


You mean shut down the company?
We need to shut down the production systems, wipe the hard drives clean, and rebuild from development files on not-externally-exposed machines. They're less likely to have time bombs planted on them.
For 3 days
How sure are we to rebuild in 3 days?
Not so sure!

*i*Premier Case - B

- *Should iPremier implement Ripley's suggestion to shut down the company and rebuild the production platforms?*

*i*Premier Case - B

- *Are there any new thoughts on what should be disclosed publicly?*

- **Now, what should be disclosed? Compose your press release.**

What is Cybersecurity Crisis Communications?

Cybersecurity Crisis Communications Phases

"those that fail to learn from history are doomed to repeat it." Winston Churchill

Source: Mandient. Google

*i*Premier Case

Part C

*i*Premier Case - C

- Disclosure –now what do we say?
- *What is your assessment of iPremier's leadership?*
- *Is anyone at fault?*
- Should anyone lose his or her job?
- *What killed this company?*

Which aspect of the iPremier case do you find most concerning?

Assignment – *i*Premier case study

Assignment Questions: Each question carries Marks.

- How well did the *i*Premier Company perform during the seventy-five-minute attack? If you were Bob Turley, what might you have done differently during the attack?
- The *i*Premier Company CEO, Jack Samuelson, had already expressed to Bob Turley his concern that the company might eventually suffer from a "deficit in operating procedures." Were the company's operating procedures deficient in responding to this attack? What additional procedures might have been in place to better handle the attack?

Assignment – *i*Premier case study

- Now that the attack has ended, what can the *i*Premier Company do to prepare for another such attack?
- In the aftermath of the attack, what would you be worried about? What actions would you recommend? Consider the prevalence and sophistication of DDoS attacks and proliferation of DDoS attack kits in the Dark web.

Note: Your response should be type written in your own words.
There is NO one right answer.
Your responses should be succinct, crisp, cogent and well presented.
All references should be cited appropriately including from AI tools like ChatGPT.

Thank you!

Follow us

isfcr.pesu

www.isfcr.pes.edu

ISFCR

PESU ISFCR

PESU Center for
Information Security, Forensics and Cyber Resilience

PES UNIVERSITY

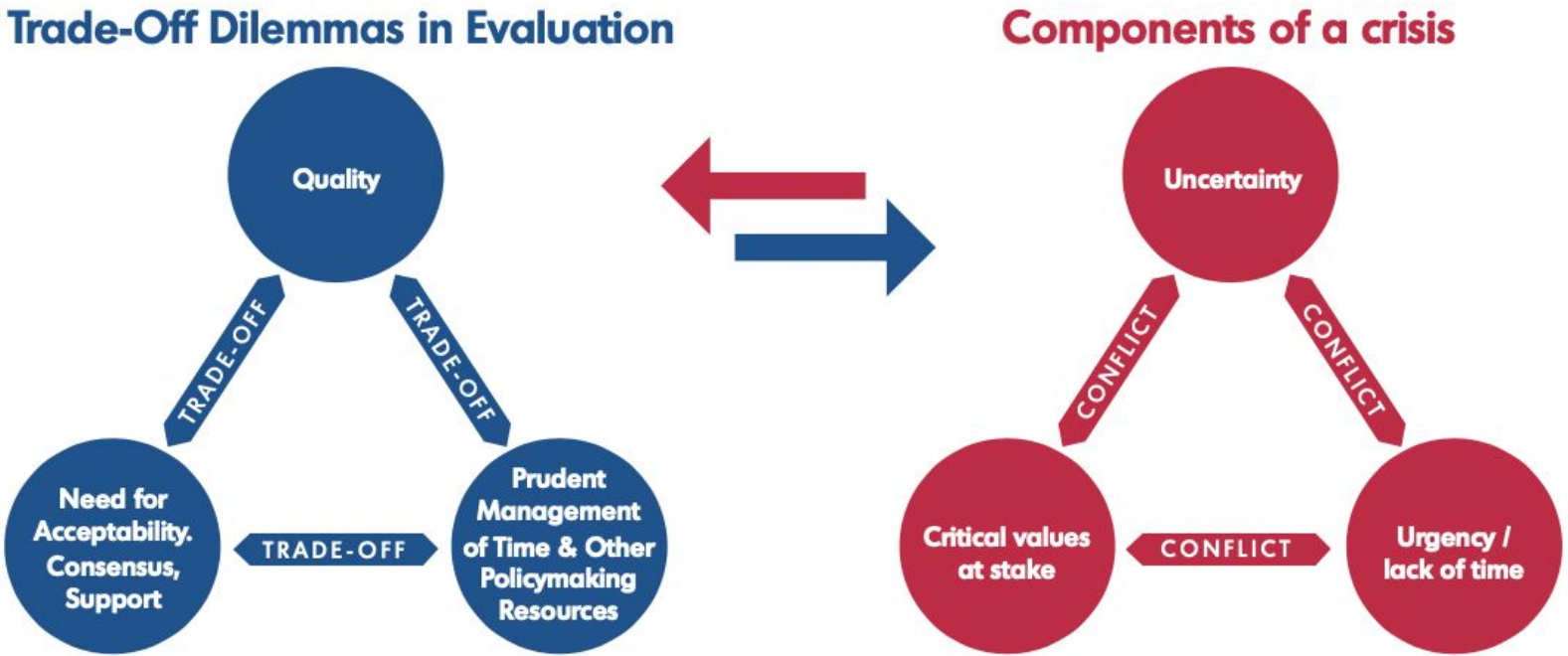
What is a Cyber Crisis?

What is a cyber crisis?

It is a situation, usually result of a Cyber attack, when one or more malicious action(s) on an Information Security cause(s) a major disruption of the entity, having various and **significant impacts, and sometimes causing irreversible damage.**

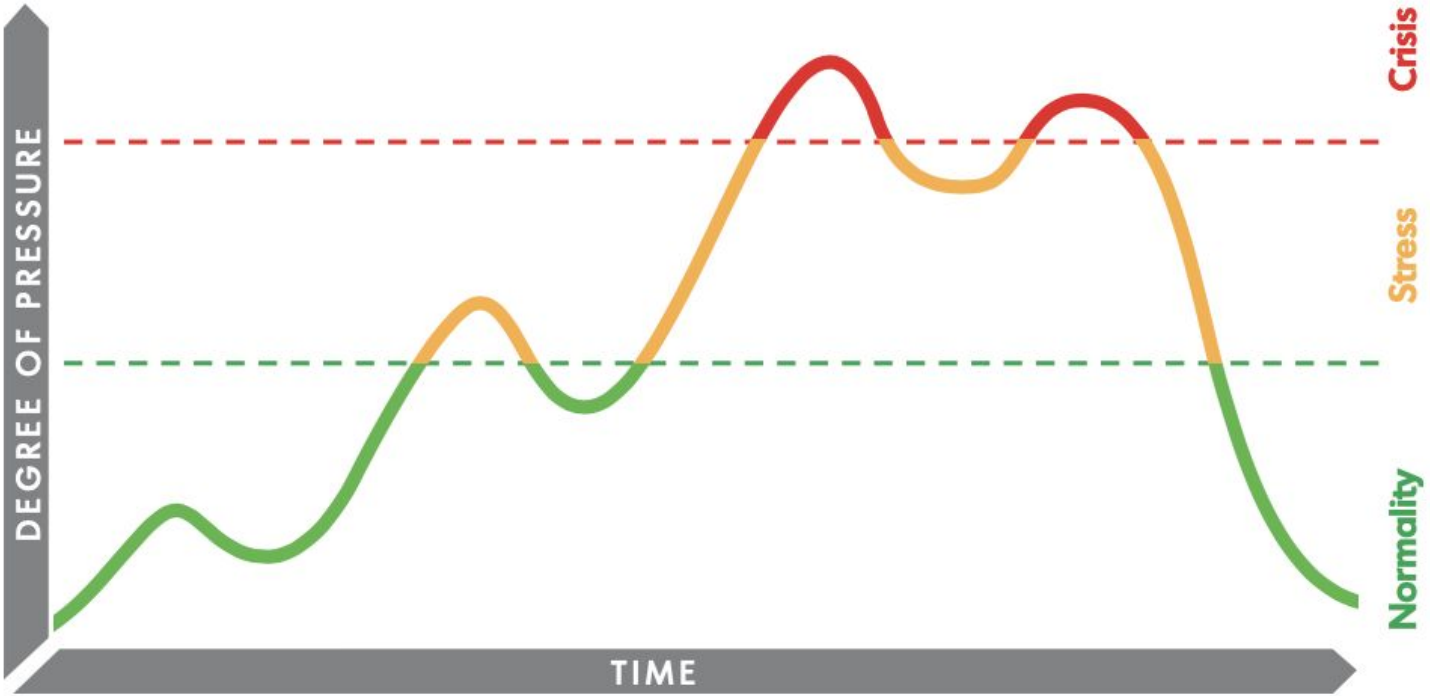
Source: European Union Agency for Network and Information Security

Characteristics of crises vs. normal decision-making



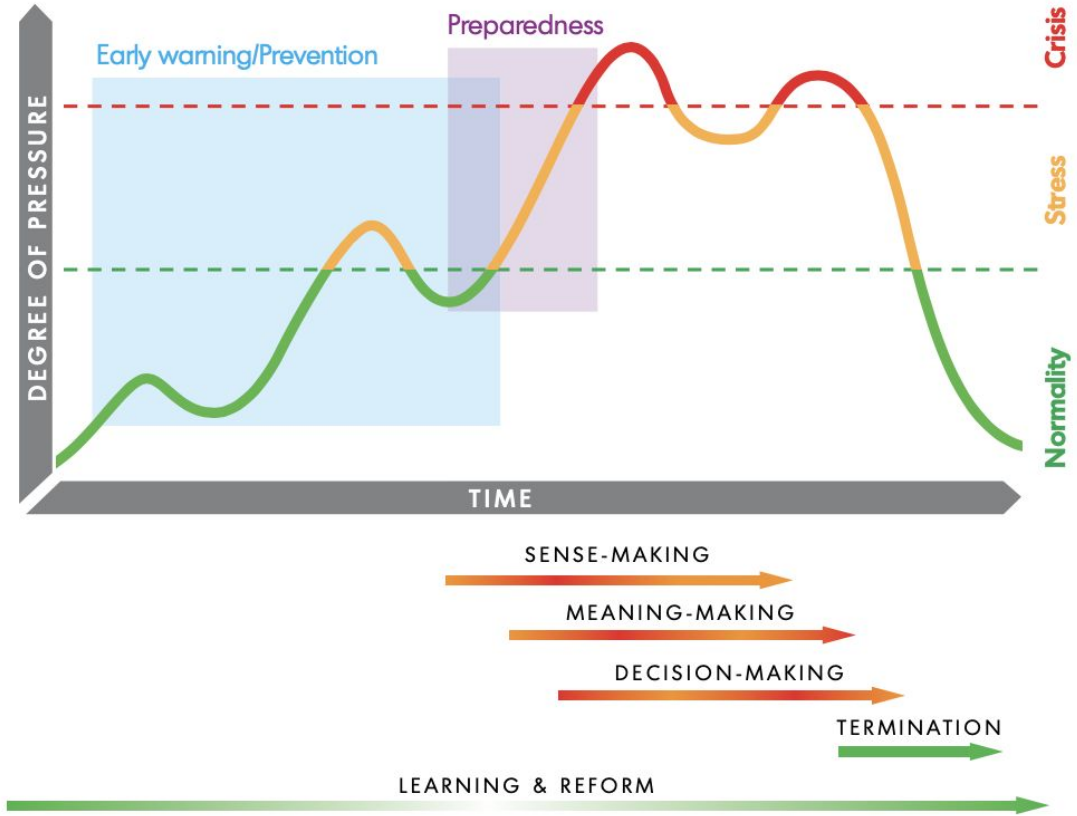
Source: Koraeus (2015). Figure is a composite of two illustrations found in the publication.

The intensity pattern of a crisis



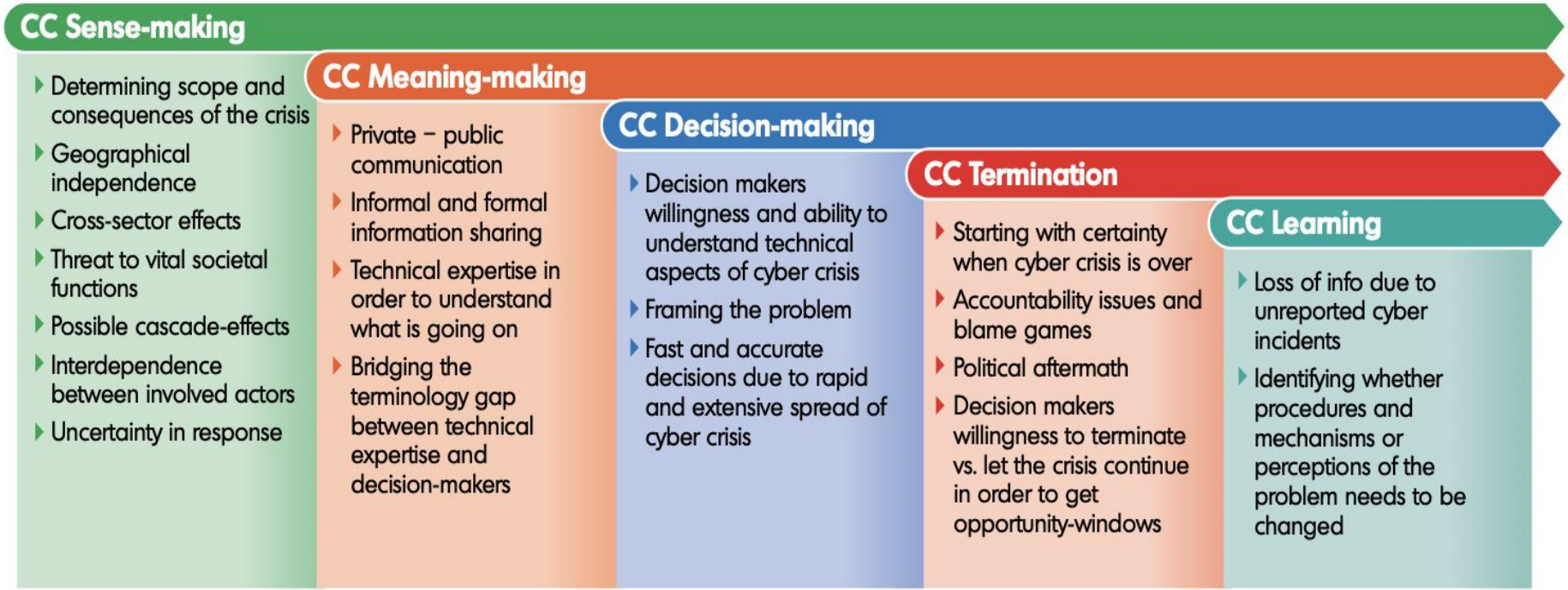
Source: Boin et al. (2005); Boin, McConnel & 't Hart (2008); Bovens & 't Hart (1996); Rosenthal, Boin & Comfort (2001).

Timing and intensity of crisis management tasks



Source: Boin et al. (2005); Boin, McConnel & 't Hart (2008); Bovens & 't Hart (1996); Rosenthal, Boin & Comfort (2001).

Cyber Crisis management challenges



Sense-making challenges:

- First and foremost, is the organisation set up to collect and respond to early-warning signals?
- Does the organisation accept that crises can actually happen, or does it suffer from a form of “it will never happen here” exceptionalism?
- How is the issue verified? Just because a problem has been detected and classified does not mean that it has been properly identified.
- If a problem is not known or familiar beforehand, it becomes much harder to detect, much less to properly identify it.
- What kinds of crises are actually allowed to be detected? Political constraints may render some issues unacceptable—the detection of such issues have the added obstacle of overcoming institutional ideology and inertia.

Meaning-making challenges:

- How is the issue framed? Labelling the same event as an accident generates a different response than if it were called a tragedy. What, then, is the desired response?
- Is messaging surrounding the crisis tailored for its audience? Making the public understand an issue is often a very different matter than making experienced practitioners understand what the chosen course of action and the reasons for doing so.
- How credible is the message? Repeatedly overpromising and under-delivering? Such actions erode trust and make it less likely that other parties will support the next critical decision.
- Is symbolic communication being used? A failure to acknowledge the emotions arising due to the crisis, of sharing shock and grief, may only convey an air of indifference and callousness, quickly eroding trust and support, exactly opposite of what is needed.

Decision-making challenges:

- How are ambiguities and uncertainties resolved? Is the organisation able to retain previous hypotheses about the situation and act on them if it turns out that the initial interpretation was incorrect?
- Non-decisions are also decisions. It is often convenient and comforting to take a “wait and see” approach, but are such decisions analysed and treated like any other course of action?
- How much actual decision-making takes place? It is very easy for plans to become scripts, removing the agility, adaptability, and improvisation that is needed to handle a crisis.
- How does the coordination work? Are the strategic goals and operational efforts in line with each other, or do they end up working at cross-purposes?
- At the same time, are the different levels of decision-making properly separated or does, for instance, the strategic level become distracted by trying to micro-manage operative matters?

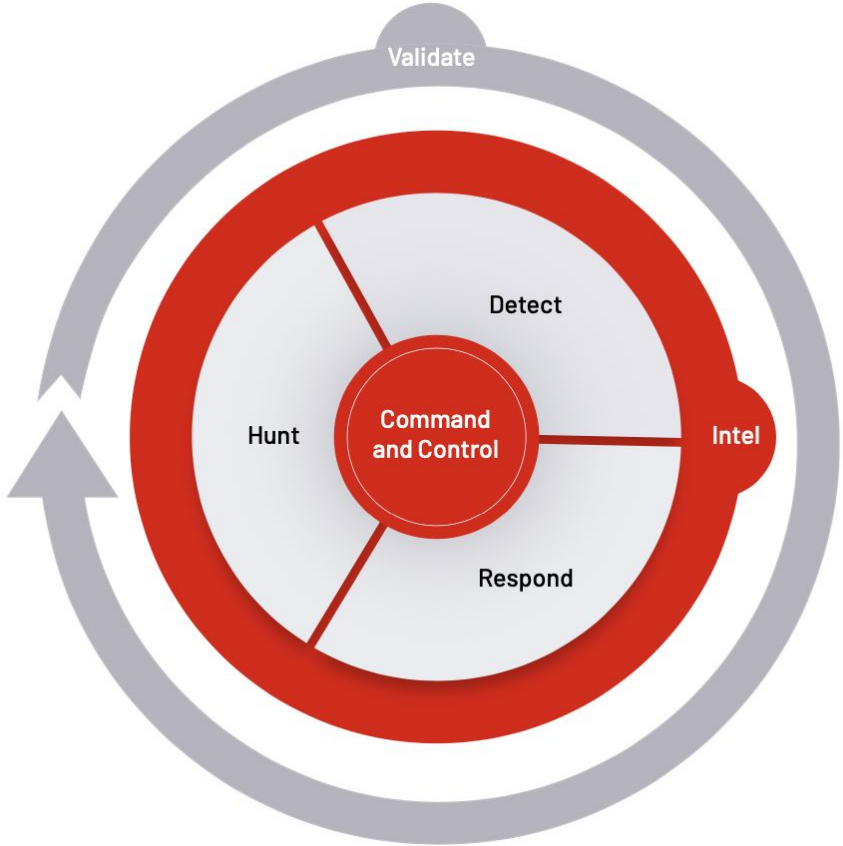
Termination challenges:

- How does one determine that the crisis is really over? Mirroring the problems involved with sense- making, it can be hard to state with any certainty that things are now back to normal.
- Terminating the crisis too late is just as bad as ending it too soon. Calling an end to crisis management only to have the crisis flare up again proves beyond any doubt that the crisis manager is not—and perhaps never was—in control of the situation. On the other hand, dragging the crisis out just gives the impression that the decision-makers are trying to profiteer on the emergency efforts and/or that the crisis is largely artificial.
- The accountability trap: the same decision-makers that were responsible for "letting the crisis happen" are now trying to take charge and say that the crisis is over. Yet how can they be trusted to make that kind of judgement call given the error in judgement just witnessed by all?
- Blame games often ensue as one party or another tries to pin responsibility on someone else inorder to score political points, to further some agenda, or to shift responsibility away from themselves in an attempt to avoid the accountability trap.

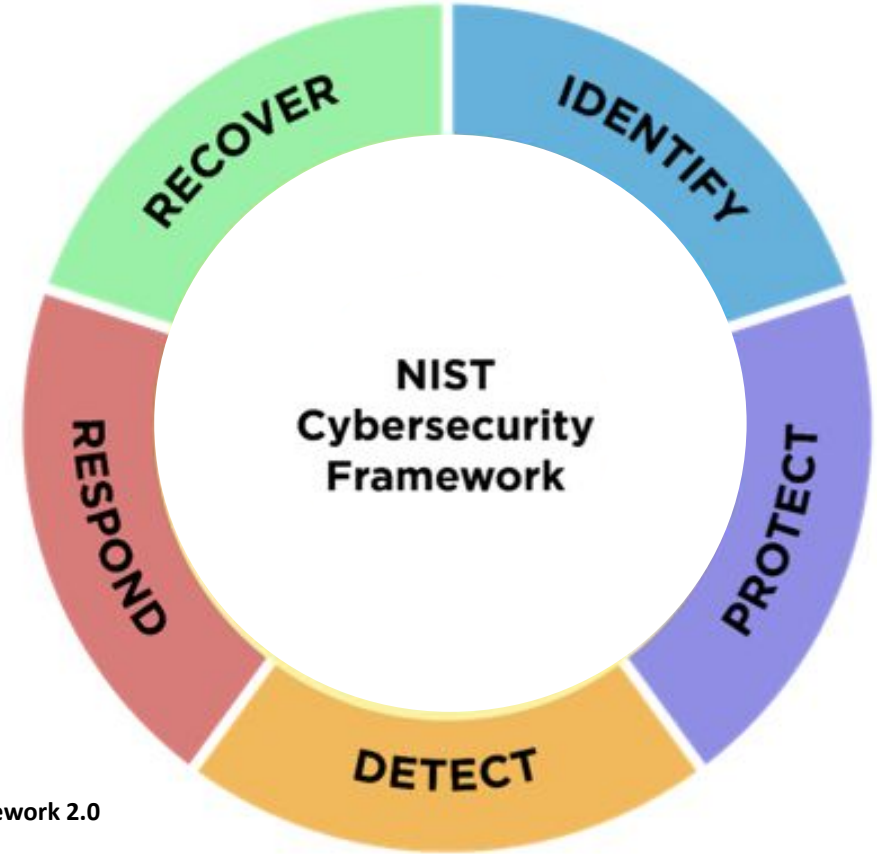
Learning and reform challenges:

- Return of the accountability trap: how does one argue for reform when the same party was, just recently, intent on returning to a state of normality that permitted the crisis to occur?
- How much of the learning actually results in tangible improvements? Many times, the supposed learning is purely a paper product: an unrealistic document that claims that lessons have been drawn and changes made, but in practical terms, everything just goes back to the way it was before the crisis.
- At the same time, learning is not the same thing as change! While there is often a strongly felt need for change, it is equally important to recognise mechanisms that worked perfectly well, and which should therefore not be needlessly swept away by reform.
- What is the lesson that actually needs to be learned? There maybe nothing wrong with the procedures and mechanisms involved, but rather with the fundamental assumptions about what kind of problems the crisis management system is meant to solve. So it is the perception of the problem that needs to be reassessed rather than the methods used in dealing with whatever problem might arise.

Functions of Cyber Defence in Action

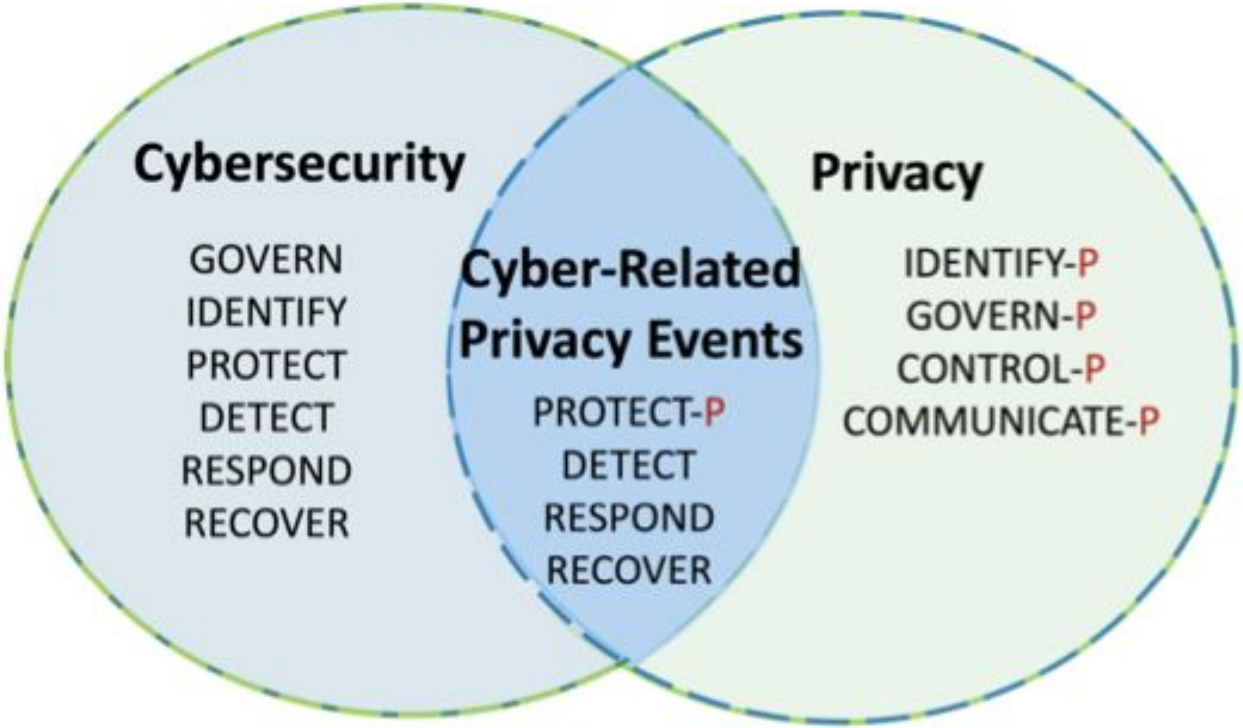


Cybersecurity Framework



Source: **The NIST Cybersecurity Framework 2.0**

Cybersecurity Framework and Privacy Framework



Source: **The NIST Cybersecurity Framework 2.0**

*P = Privacy Framework

Cybersecurity Framework – Function n Category

Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Cybersecurity Supply Chain Risk Management
	Roles, Responsibilities, and Authorities
	Policies, Processes, and Procedures
	Oversight
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience

Function	Category
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

Domains of Information Security

Elements of Cyber Defence

Intelligence

Guiding Light

Hunt

Threat Hunting and
Compromise Assessment

Respond

Incident Response
and Recovery

Command and Control

Maintain the Mission

Detect

Alert Monitoring
and Investigation

Validate

Targeted Testing
and Controls Validation

Relevant CIS Controls for iPremier

CIS Control	Description	Relevance to iPremier	Exercise Ideas
5. Account Management	Manage accounts, roles, and permissions.	iPremier had unclear access and no defined ownership of systems during crisis.	Design an access control list showing who should access logs or systems during incidents.
8. Audit Log Management	Collect and monitor logs for anomalies.	The company relied on its ISP for logs, showing lack of visibility.	Use sample web logs (lab) to detect abnormal traffic patterns.
13. Network Monitoring and Defense	Deploy IDS/IPS and monitor network traffic.	iPremier had no network intrusion detection system or DDoS mitigation.	What tools or architectures (like CDNs, WAFs, scrubbing services) could have mitigated this?
17. Incident Response Management	Develop, test, and refine incident response plan.	No documented IRP; leadership was unprepared.	Create a 1-page IR plan with roles and escalation steps.

Example – Shared Intel

- Managed detection and response services team
  - Received information about a zero-day vulnerability in a widely used product being exploited to deploy ransomware.
  - The managed service provider initiated a threat hunting campaign to identify evidence of attacker activity across the entire customer base.
  - Additional intelligence led the managed detection and response services team to begin scoping customer environments for hosts running the vulnerable software.
- Affected customers were quickly identified and advised to contain certain on-premises systems.
  - Protections were put in place before the ransomware could be deployed.
- In this case, all customer of managed services and other SaaS offerings benefited from the adversary IOCs (indicators of Compromise) provided from intelligence gathered across the customer base.

A basic threat intelligence Plan

Creating actionable intelligence starts with creating a threat intelligence plan.

A basic threat intelligence use case plan needs to answer the following questions:

1. What is to be accomplished?
2. Who will consume the intelligence output?
3. How will the intelligence output be communicated?
4. How will feedback on the output be gathered and consumption measured?
5. What additional intelligence sources are needed to fill existing gaps?

Command and Control responsibility

- The Hunt function develops and executes a campaign that uncovers activity matching known IOCs tied to a potential high-risk exploit that has recently been made public within the industry.
- To ensure that the Detect function develops detection criteria for use cases to identify and alert on potential activity tied to the IOCs.
- In addition, it is the responsibility of the group to ensure that the Respond function has the appropriate response procedures documented to react to a compromise as quickly and efficiently as possible.
- These efforts should be identified and tracked to completion to ensure that the organization is properly prepared for the threat before the environment is impacted.

Detect

As this is an engineering discipline, practitioners execute in an iterative fashion:

1. Identify the organization's adversarial value.
2. Select a known threat actor likely to target the organization.
3. Profile the behavior of the threat actor.
4. Identify the threat actor's TTPs.
5. Determine measurable impact of each TTP to the system.
6. Implement visibility to showcase the measure.

Detect

As this is an engineering discipline, practitioners execute in an iterative fashion:

7. Qualify the measurement's fidelity.
8. Set alert thresholds.
9. Design and build the alert.
10. Test, validate, and integrate the alert into the production environment.
11. Review triggered alerts for accuracy and calculate its value.
12. Sustain, enhance, or dispose of the alert based on the review findings.

Example – VPN Compromised Credentials

- An adversary who used compromised credentials against the organization's VPN access was discovered.
- The organization detected account abuse when the adversary emailed the help desk asking for a password reset, the help desk responded, and the actual user reported the impersonation.
- With this alert, the initial evidence was limited to the IP address and the account used by the adversary.

- **The investigation team began with three questions:**
  1. What other activity has been seen from this IP address?
  2. What sensitive systems and data did the compromised account have access to?
  3. What did the adversary do with this account?

Example - VPN Compromised Credentials.. contd

- These questions inform the analysts what artifacts and evidence they need to seek out.
  - By examining VPN logs and firewall logs they found other compromised accounts and access to the organization's web facing email.
  - By examining security groups and access control lists, they determined the first compromised account had access to a sensitive file server mounted as a network share to one of the accessed endpoints.
- By leveraging user activity artifacts, they found the adversary broadly searching for documents using queries such as *.pdf, *.xls, *password*.
  - At this stage, the attacker did not use keywords and phrases relevant to the organization's name, sensitive projects, or key personnel.
  - The untargeted queries intimated that the attackers were still in an information gathering phase or that this was possibly an opportunistic attack.
  - Opportunistic attacks like these are more likely to be monetized by various means, such as selling access to another attacker or ransomware.

Example - VPN Compromised Credentials.. contd

- By profiling the attacker, the observed tooling and the adversary's current control, ransomware did not appear likely although data theft was seen
- In addition, this threat actor did not immediately pursue domain admin permissions or privilege escalation
- They kept the systems they accessed focused on low-privileged users who had access to file shares.
- When specific intelligence is available, the next steps can be quickly developed based on the threat actor's habits and practices. Otherwise, defenders must rely on generic intelligence, surmising the adversary's objectives along the way.

A critical question that must be asked regularly is, "Does this make sense?"