<https://www.youtube.com/watch?v=yZtm7yZAm7o&feature=youtu.be>

**🧑‍💼 The Role of Senior Management, Cyber CPR, Short-Term Strategies, and RTIR**

**🧠 1. The Role of Senior Management in Cybersecurity**

**🧑‍💼 Who is Senior Management?**

People like:

* CEO
* CIO (Chief Information Officer)
* CISO (Chief Information Security Officer)
* CTO
* Department Heads

**🎯 What’s Their Role During Cyber Incidents?**

| **Responsibility** | **What it Means** |
| --- | --- |
| ✅ **Leadership** | Make fast, smart decisions in a crisis |
| 💬 **Communication** | Inform staff, customers, partners, media |
| 💰 **Resource Allocation** | Approve money, tools, people needed to respond |
| 🧾 **Compliance** | Ensure laws, policies, and regulations are followed |
| 🛡️ **Support CSIRT** | Empower the technical team to act quickly |
| 📢 **Public Messaging** | Handle PR and control reputation damage |

📌 Senior Management must stay **calm, decisive, and informed** during cyberattacks.

**🚑 2. What is Cyber CPR?**

Cyber CPR = Cyber Crisis Preparedness and Response  
It’s like **First Aid for Cyber Incidents**

Just like CPR keeps a human alive before medical help arrives, **Cyber CPR** is the **first action** to **stabilize a company during a cyberattack.**

**🔧 Cyber CPR Involves:**

1. **Identify** the breach quickly
2. **Stop** further damage (disconnect affected parts)
3. **Alert** your incident response team (CSIRT/SOC)
4. **Preserve** evidence (don’t wipe anything!)
5. **Communicate** internally and externally
6. **Execute playbooks** and plans
7. **Stay legally compliant**

✅ It’s a **repeatable checklist/playbook** that helps reduce confusion in chaos.

**🧯 3. Short-Term Cybersecurity Strategies**

These are **immediate actions** to reduce damage:

| **Strategy** | **Action** |
| --- | --- |
| 🧱 **Isolate Systems** | Cut off infected machines to stop spread |
| 🔁 **Switch to Backups** | Restore clean versions of affected systems |
| 👥 **Activate Incident Team** | Put CSIRT or SOC into action |
| 🔐 **Reset Passwords** | Especially for critical accounts |
| 🚫 **Block Malicious IPs/Domains** | Use firewall or IDS/IPS rules |
| 📞 **Communicate** | Keep employees and leadership in the loop |
| 💼 **Engage Legal & PR** | Prepare statements and handle legal duties |
| 🧾 **Document Everything** | Helps in investigations and legal compliance |

**🛠️ 4. RTIR – Request Tracker for Incident Response**

RTIR = **Open-source ticketing system** made for managing cybersecurity incidents  
**Built on:** RT (Request Tracker)  
**By:** Best Practical

**🎯 Why Use RTIR?**

It helps teams track:

* 📥 Incoming alerts or suspicious activity
* 🔍 Investigation steps
* 🛠️ Actions taken (containment, recovery)
* 📄 Reporting and documentation

| **Feature** | **Benefit** |
| --- | --- |
| 🎟️ Tickets | Every incident is organized as a ticket |
| ⏳ Timelines | Helps track response time and deadlines |
| 📂 Templates | Use forms for fast data entry |
| 👥 Collaboration | Teams work together on one platform |

✅ RTIR helps improve **speed, structure, and communication** during incident response.

**📘 Summary Table**

| **Topic** | **Key Points** |
| --- | --- |
| 👨‍💼 Senior Mgmt | Lead, communicate, allocate resources during incidents |
| ❤️ Cyber CPR | First-response actions to stabilize systems during attack |
| 🛡️ Short-Term Strategies | Quick fixes: isolate, reset, block, backup |
| 🧾 RTIR | Ticket system to manage incident response activities |