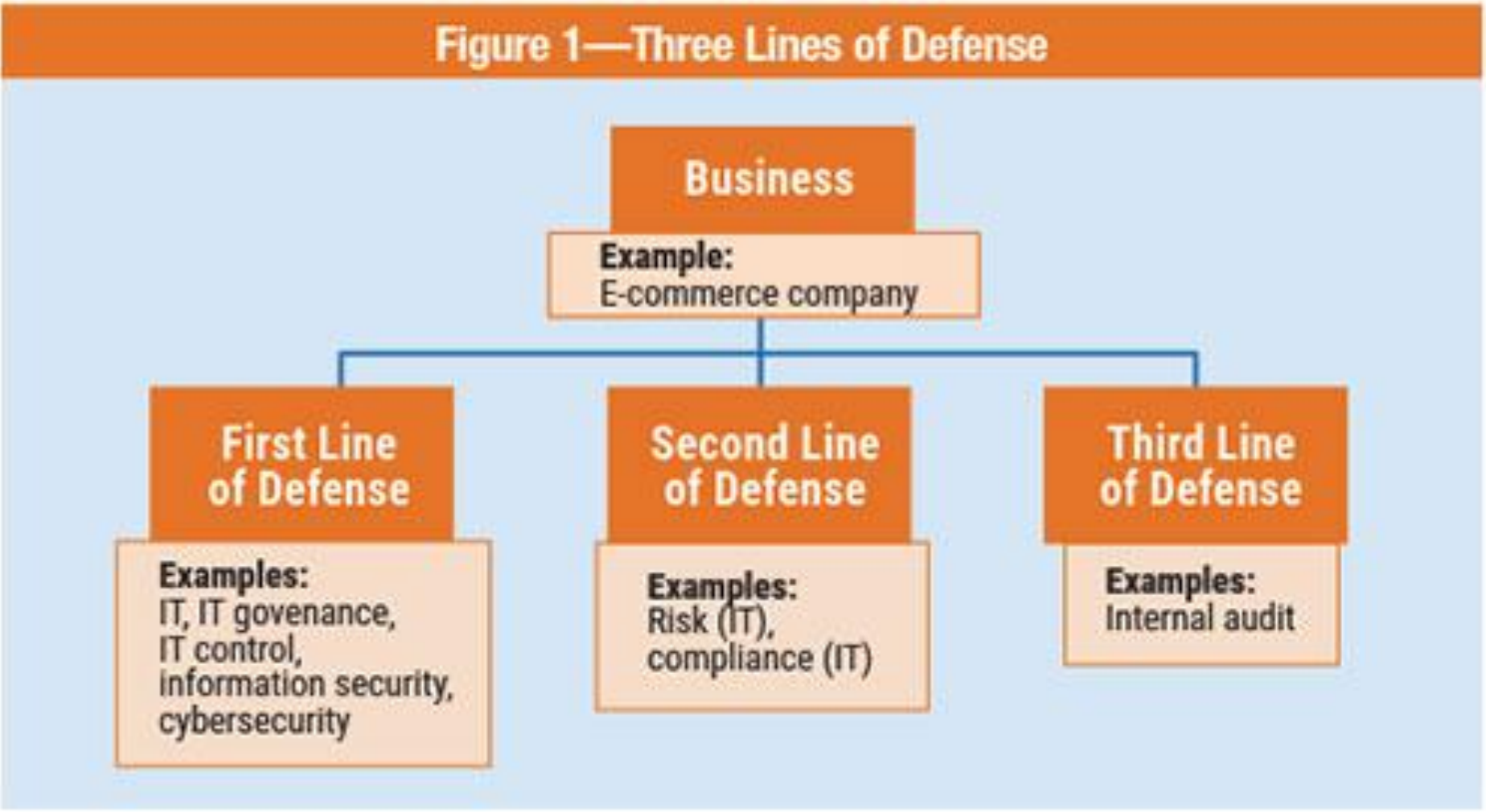
BY- SAMIKSHA BISHT

CYBER SECURITY

Content

- Enterprise roles and functions
- Information security roles
- Position alternatives
- Enterprise structures and interface

Line of defense



Enterprise Roles

- **First, Every team member understands the importance of their role.** Everyone on the team needs to be focused and performing well *every single day to be effective* — and they need to understand *why* that is so important.
- **Second, security is there to facilitate the business, *not* to work against the business.** If even one member of your team takes on a "no can do" attitude for every management request, that will throw off the rest of the team. Emphasize to every team member that their job is to help the business find the most secure way to accomplish the need — security and the business should be partners.

Responsibilities

- **1. Software Development**
- Having someone on your team with secure software development skills is a huge advantage for a cyber security team. Many companies rely on external third parties for development, but it really helps strengthen a security program to have someone on board with the knowledge and skill set to be part of those conversations.

Contd.

- **Finally, it's critical not to overstate risk, but to keep the discussion logical and fact-based.** As Celia Baker, President of the IntelliGRACS Group Inc., told us, "If you're going to say the sky is falling, be sure it's *really* falling — not just starting to rain." Some security professionals may be tempted to craft dramatic cyber security messages based on FUD (fear, uncertainty, and doubt) to secure funding or make a point. That may work once or twice — but in the long term, management will stop listening. Ensure that every team member keeps their presentations solid and fact-based as risk is being communicated up the chain and across the business.

Contd.

- **2.Threat Intelligence, Intrusion Detection, & Incident Management**
- Key to cyber security are monitoring and identifying issues before they happen, catching issues as quickly as possible, and taking the necessary steps after an incident has taken place — you'll need team members who can handle these discrete but connected functions.
- **5. Risk Mitigation**
- Every member of your team should understand how to mitigate risk. It's helpful here to have team members that understand controls and auditing. If you can think like an auditor, you can identify weak controls (cause risk) and then implement appropriate risk mitigation strategies.

Contd.

- **6. Data Analytics**
- Do you have someone on your cyber security team who can look at raw data to identify patterns and cull out useful and actionable information? Knowing and understanding how to correlate and interpret data is critical for cybersecurity. If not, you need to be sure you hire for this or foster this skill as soon as possible.

Contd.

- **7. The Ability To Work Across The Organization**
- More of a soft skill, this is still critical for every cyber security team member. You can have very intelligent team members with top-notch security skills, but if these individuals can't have relevant conversations with people in other departments in a manner that elicits cooperation, they'll have more limited career opportunities, limited effectiveness in their current roles, and less opportunity for advancement. Not being able to speak the language of the business and other teams is a primary reason good technical people don't advance beyond middle management. So be sure every team member knows how to work and communicate with other teams and other levels of management — knowing how to explain technical things in simple terms to non-technical people will go a long way.

What is information security

- Information security is a set of practices intended to keep data secure from unauthorized access or alterations. Here's a broad look at the policies, principles, and people used to protect data.
- Information security, sometimes abbreviated to *infosec,* is a set of practices intended to keep data secure from unauthorized access or alterations, both when it's being stored and when it's being transmitted from one machine or physical location to another.

Roles of Cyber Security

- Information security performs four important roles:
- Protects the organization's ability to function.
- Enables the safe operation of applications implemented on the organization's IT systems.
- Protects the data the organization collects and uses.
- Safeguards the technology the organization uses.

Contd.

- Our CyberComply platform guides organizations through cyber risk and privacy monitoring and compliance. It's designed for risk and security, data and compliance, and IT and information security professionals working in small- and medium-sized organizations for which cyber risk and privacy management are critical.
- It has been developed to:
- Be **scalable** to address evolving and increasing threats;
- Be **repeatable** for frequent risks assessments;
- Reduce **variability** by helping you make consistent decisions based on fact rather than human interpretation;
- Be **maintainable** for multiple stakeholders across your organization; and
- Have **everything you need in one place** for governance, risk and compliance, making it a **quick and cost-effective** route to compliance.

ENTERPRISE INFORMATION SECURITY ARCHITECTURE (EISA)

- Developing a high-level information security (InfoSec) infrastructure for your organization takes plenty of time and manpower. If you're not devoting the appropriate efforts to securing your network data, it will most likely be compromised in some way shape or form. It is for this reason why building and nurturing an Enterprise Information Security Architecture (EISA) from idea to creation.

Contd.

- **Why are Enterprise Information Security Architectures (EISAs) Beneficial to Your Bottom Line?**
- Enterprise Information Security Architectures (EISAs) are fundamental concepts or properties of a system in its environment embodied in its elements, relationship, and in the principles of its design and evolution. They are fundamental concepts and properties of a system that establish the purpose, context, and principles that provide useful guidance for IT staff to help make secure design decisions. EISAs also define the environment and relationships that it exists in, while also doing some deep digging into the concepts and imagination of a system.