**Security incident analyst. Best practices.**

**Cybersecurity policy.**

Cybersecurity policy must be created since the company established and basics paragraphs must be known all employee, include partners(outstaff). Every year the policy must be improved and reviewed because the company faced with new conditions on their business. Every employee read the policy and put the signature in the familiarization log. Every year, HR specialist should create some interactive tests for all employee, get all results and send results to the Security officer.

**Security staff.**

Every enterprise company should have enough security staff. They should consist of cybersecurity engineers(80%) and physical security officers(20%). The responsibility about cybersecurity should be divided between all security staff. One part should be responsible of security about business applications, critical applications and network, and second part should protect servers and communications boxes.   
Also, security officers should protect physical access to the main and branch offices.

**Continues learning**

As I have written before, every year HR department must conduct various training and education.  
Every training course mandatory has a part about cybersecurity which depended with header of course.  
Security check each other are welcomed. Every lead should speak about security rules with every team member.

**General communications**

The chief security officer should make research about new threats and vulnerabilities and write a letter for all staff about them with description how minimize impact and protect your work. There are many security communities, articles and magazines which help security staff to be deep in security world and made their job more effective. Subscription on this materials are mandatory.