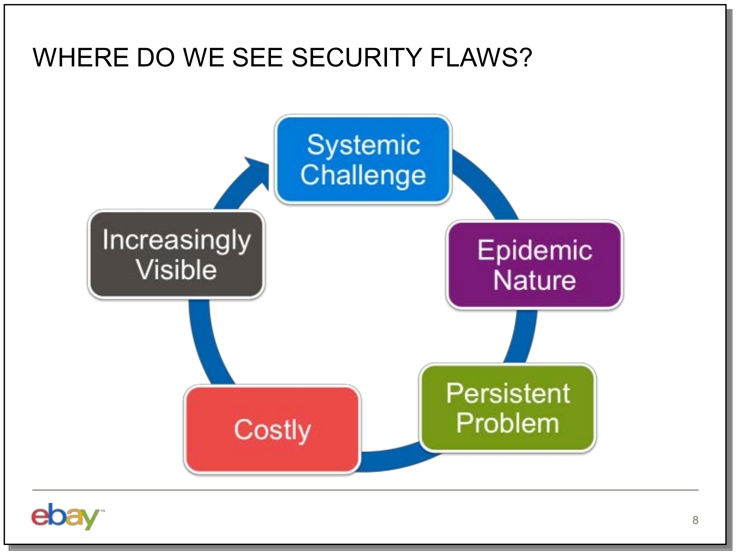
Slide 8



WHERE DO WE SEE SECURITY FLAWS?

Systemic Challenge

Epidemic Nature

Persistent Problem

Costly

Increasingly Visible

8

One thing we know about security flaws is that they are **systemic**. Security flaws can be introduced at any phase of the development process, in both Agile and waterfall processes.

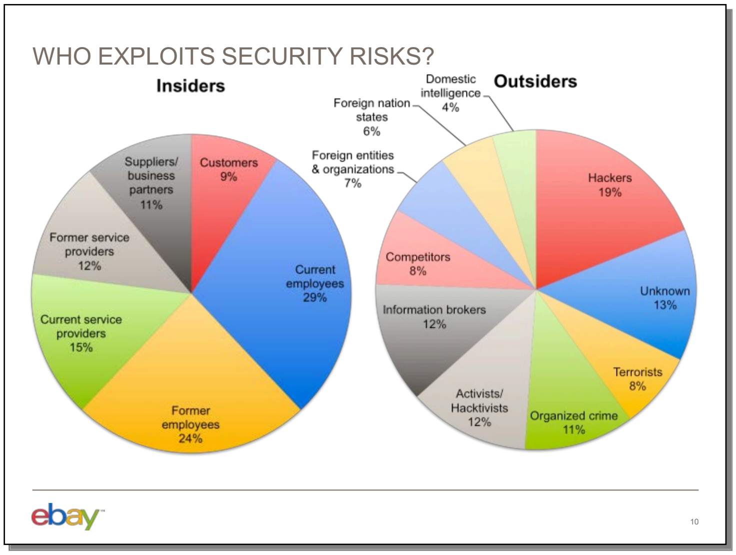
Security issues are **epidemic**. They can exist in any programming language, on any type of device, in any country around the world. A recent study of more than 9,700 security, IT, and business executives found that the total number of security incidents detected by respondents had climbed to 42.8 million, an increase of 48% over 2013. That’s the equivalent of 117,339 incoming attacks per day, every day.

Security is a **persistent** issue. We also know that we must continually work to prevent and resolve security issues, or they will continue to occur and to persist in production.

Security issues have a **costly impact**. And just like any other type of system defect, the later the security issue is identified, the more expensive it is to fix. And when we are busy fixing defects, we are not able to innovate, so there are additional costs relating to lost opportunities for all the things that we did not have the time or money to develop. Globally, the annual estimated reported average financial loss attributed to cybersecurity incidents was $2.7 million, a jump of 34% over 2013. Organizations reporting financial hits of $20 million or more increased 92% over 2013.

We also know that security issues can be highly **visible** and can subject a company to much unwanted publicity.

Slide 10



WHO EXPLOITS SECURITY RISKS?

We are vulnerable when an attacker has both access to a security flaw and the capability to exploit that flaw.

Hackers and criminals are not the only ones who can get that access or develop those capabilities. Thus they are not the only ones who can exploit security flaws and cause harm to eBay and our customers. According to some industry reports, a third of all cybersecurity lapses are caused by insiders such as current and former employees, service providers, and suppliers. This makes sense because these people already have access – or know how to get it – and capability – or can develop it.

So if we really want to improve security, we have to consider the entire development process – we can’t just focus on what is in production.