

Module 1

Global picture of modern threats in Cyber Security

Goals & Objectives

The goal of this module is to provide an understanding of the variety and complexity of threats in the current enterprise IT environment.

After completing this module, you should be able to understand:

- A high-level overview of recent major incidents and the worldwide modern threat landscape, based on data and figures from IBM's X-Force Threat Research.
- Additional use cases of related concepts such as organized cyber crime, cyber crime on demand, Advanced Persistent Threat attacks, and the Cyber Kill Chain approach.
- The tools and techniques used by attacks, reviewing such concepts as Vulnerability, Exploit, and Remediation; DDOS, SQL Injection, Watering Hole attacks, Insider threat, and Zero Day attack.

Security Events, Attacks, and Incidents

These figures are averages representing single organization's security monitoring results. *Every organization is constantly under attack.*

Average annual security events, attacks and incidents



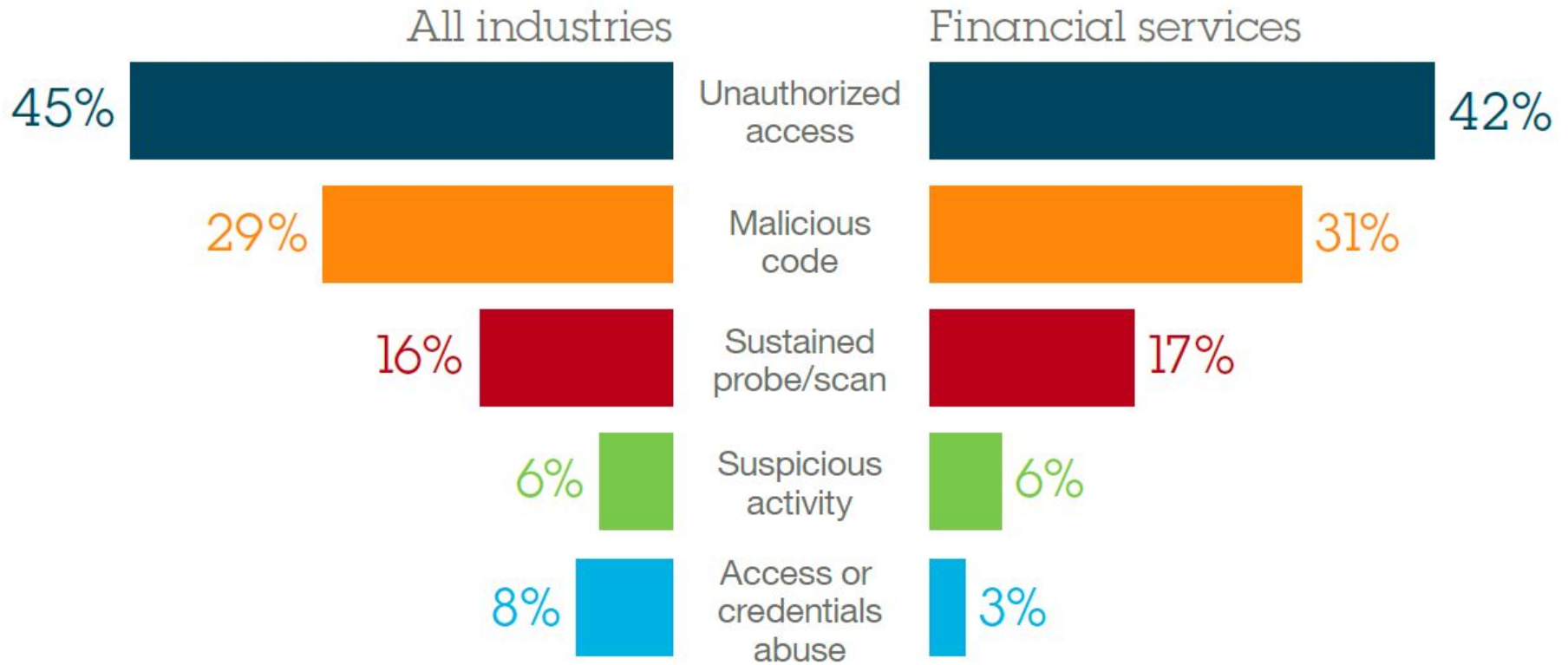
Security event: An event on a system or network detected by a security monitoring device or security application.

Attack: A security event that has been identified by monitoring tools as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy systems or information.

Security incident: An attack or security event that has been reviewed by security analysts and deemed worthy of deeper investigation.

Types of Security Incidents

Nearly half of security incidents in 2015 were the result of unauthorized access



Who is responsible for attacks?

Sixty percent of all attackers are “insiders” - and this number is increasing

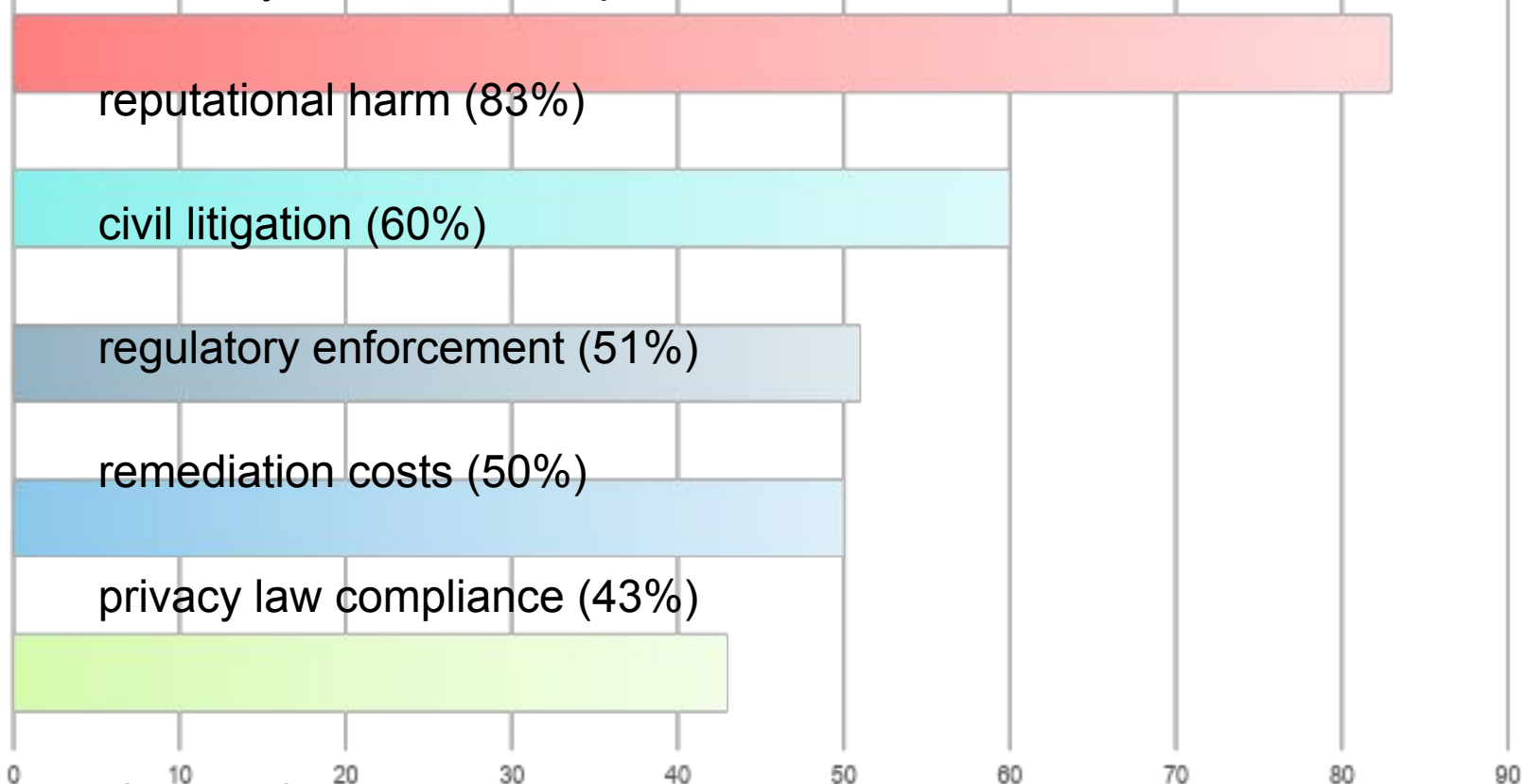


Security measures must be able to address the insider threat – as well as protecting against malicious outsiders

Cyber Risk Factors

What are the biggest risk factors from a cybersecurity incident?

A recent survey of over 100 corporate disclosure documents shows us the risks:



Each of these factors can result in significant costs to an organization.

Basic Security Concepts

Some security terms which we will be using throughout this course

Vulnerability

Any feature of a system which can be used to perform unauthorized actions, or allows bad things to occur

Exploit

A tool, program or action which is used to take advantage of a vulnerability

Asset

Anything we are trying to protect: information, people, infrastructure, or systems

Threat

What we are trying to protect against -- the possibility that a certain type of negative event may occur

Risk

The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability

Remediation

The work that needs to be done to correct a vulnerability or reduce the likelihood of a threat occurring

Threat Actors

Disgruntled employee



Hacker collective



Lone hacker



Organized cyber crime



Cyber warfare



Common Types of Attacks

These terms are commonly used to refer to standard types of attacks:

DDOS	A DDOS (Distributed Denial Of Service) attack occurs when an attacker uses many other computers to flood the target system with network traffic, making it unusable.
Phishing	Emails which attempt to deceive the recipient into taking an action. <i>Spear phishing</i> refers to personalized emails sent to highly placed recipients who are likely to have privileged access.
Malware	Any software designed to cause harm
Password attacks	An attempt to guess or deduce the password of a user
Man-in-the-middle	An attack which attempts to intercept communication between a user and a target system – often done through wifi
Insider threat	Any event in which an employee uses their access for an attack
SQL Injection	An attack which uses input on an online form belonging to the target to execute code on a target database
Zero Day	Exploit software which is used before the vulnerability is known
Advanced Persistent Threat	A threat which can use multiple exploits over a long period of time – a well-funded attack on a specific target chosen in advance

Understanding the Cyber Kill Chain

The cyber kill chain is a phase model of how attackers operate:



Identify and Reconnaissance (“Recon”)	Choosing and gathering information about the target system – usernames, passwords, email addresses, and technical features, in order to find a vulnerability
Initial Attack (“Break In”)	Exploiting a vulnerability to gain some sort of access to a machine on the target’s network
Command and Control (“Latch On”)	Once the exploit is successful, malicious software is installed on the target, the attackers establish contact with it and now control that machine
Discover and Spread (“Expand”)	Now that the attackers are inside the target network, they can explore it, find new vulnerabilities, and exploit additional systems until they find the data they want
Extract and Exfiltrate (“Exfiltrate”)	The attackers use their access to accomplish their goal – packaging the data they want and moving it to their own systems

The Cybercrime Ecosystem

Cybercrime services and tools – available on demand

