Adapting to evolving cyber attack scenarios: a focus on hacking and malware threats targeting financial applications

Marco Morana
Global Industry Committee
OWASP Foundation
Email: marco.m.morana@gmail.com
Twitter: marcomorana

OWASP

E-Crime Congress Meeting
25th October 2012, London UK

OWASP

The Open Web Application Security Project

http://www.owasp.org

Presentation Agenda

PART I: The evolution of the threat landscape for hacking and malware, the impact of data breaches and online fraud

PART II: How to adapt application security measures, activities and security tools to protect web applications from hacking and malware threats

PART III: What the future holds as the cyber threat landscape continues to change: processes, skills, tools and techniques that can support enterprise security strategy

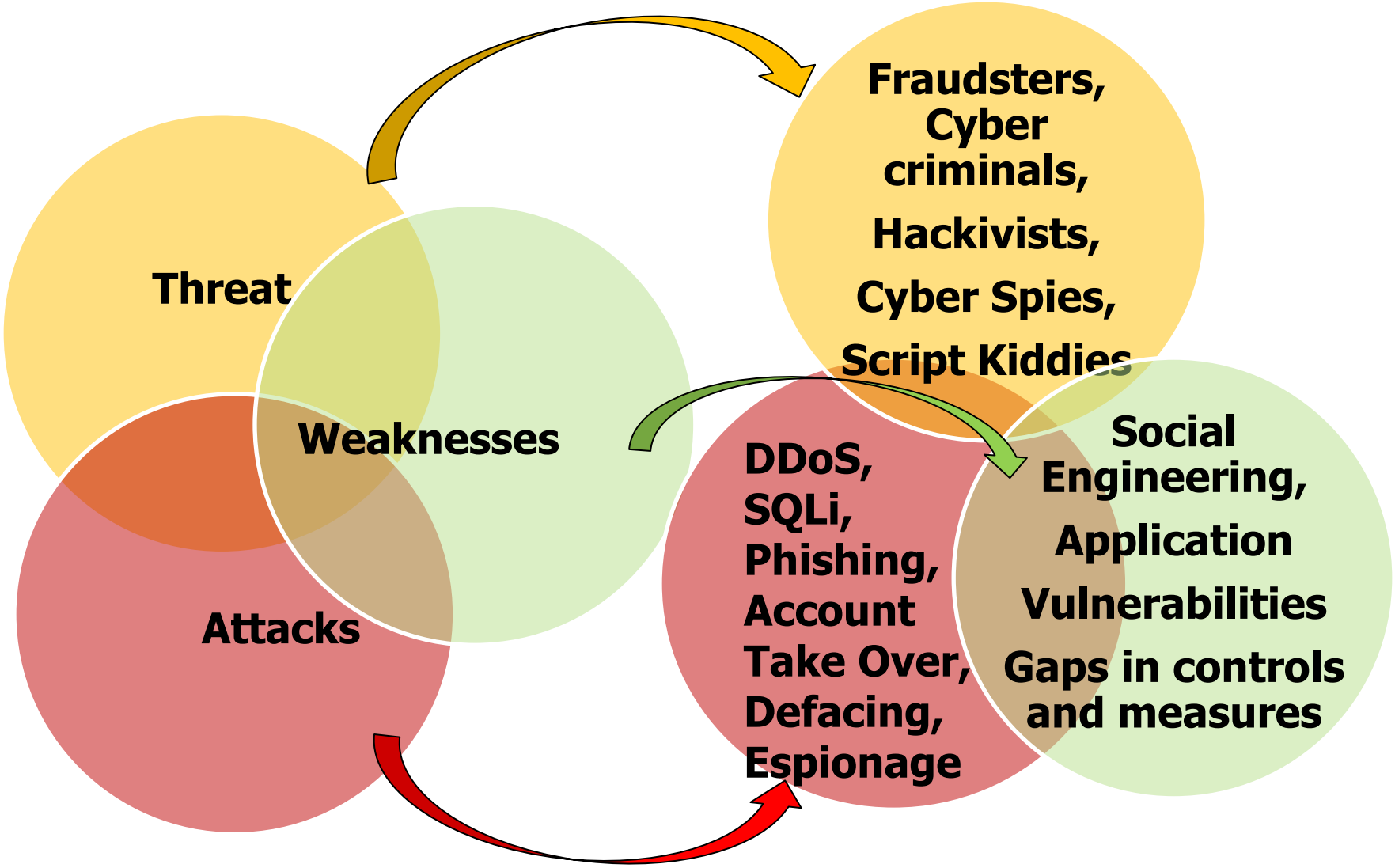
PART I

The evolution of the threat landscape for hacking and malware and the impact of data breaches and online fraud

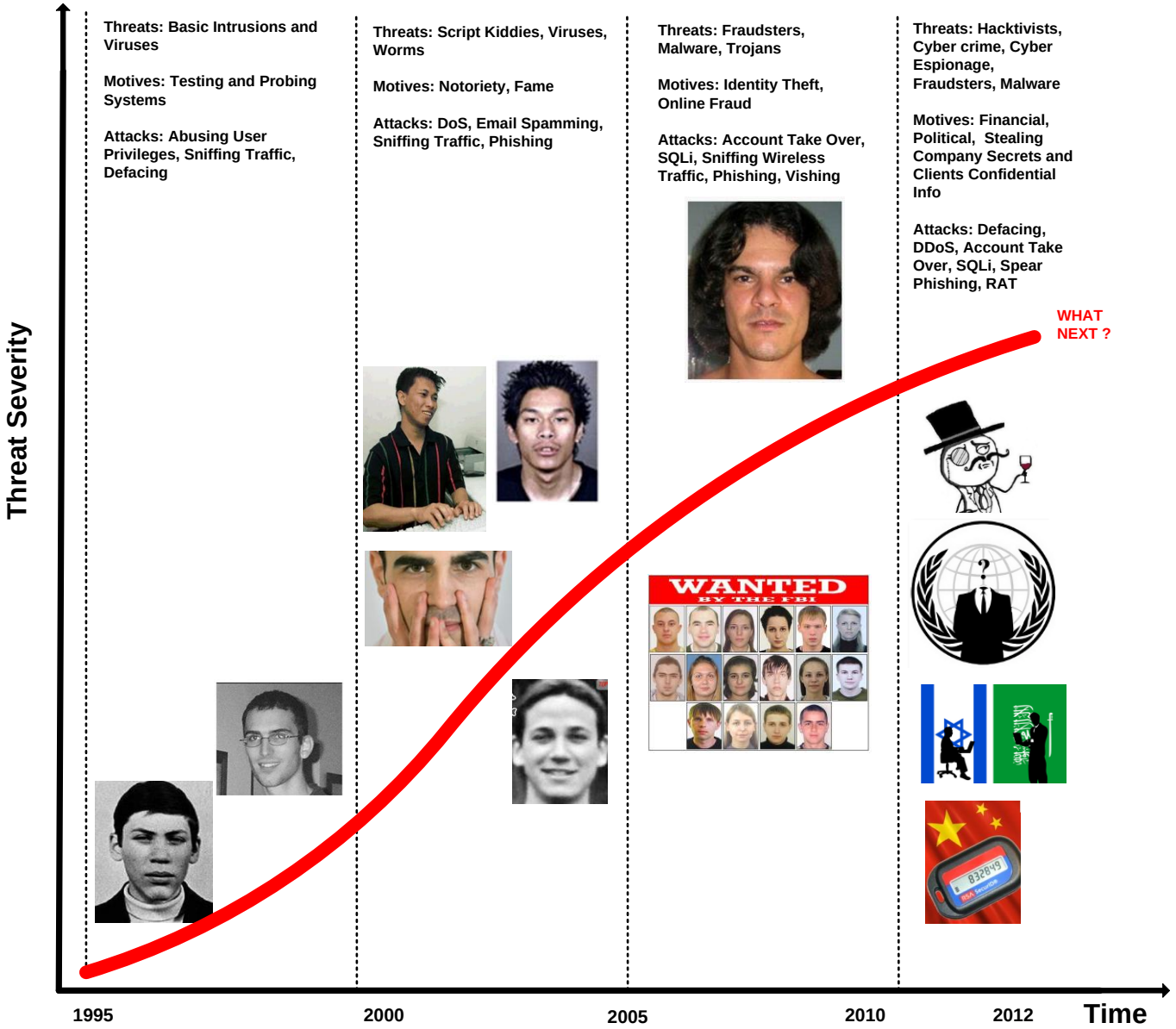
"If you know your enemy and know yourself you need not fear the results of a hundred battles"

Sun Tzu

Dissecting Hacking and Malware Threats



The Evolution of Cyber Threats



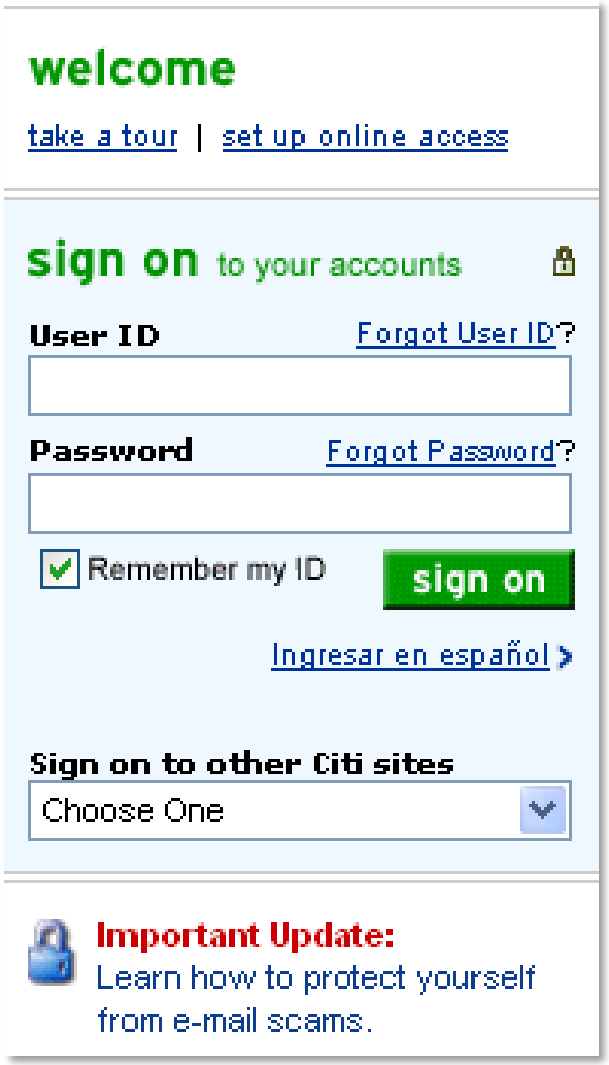
Data Breach Incidents: 2011-2012 Statistics

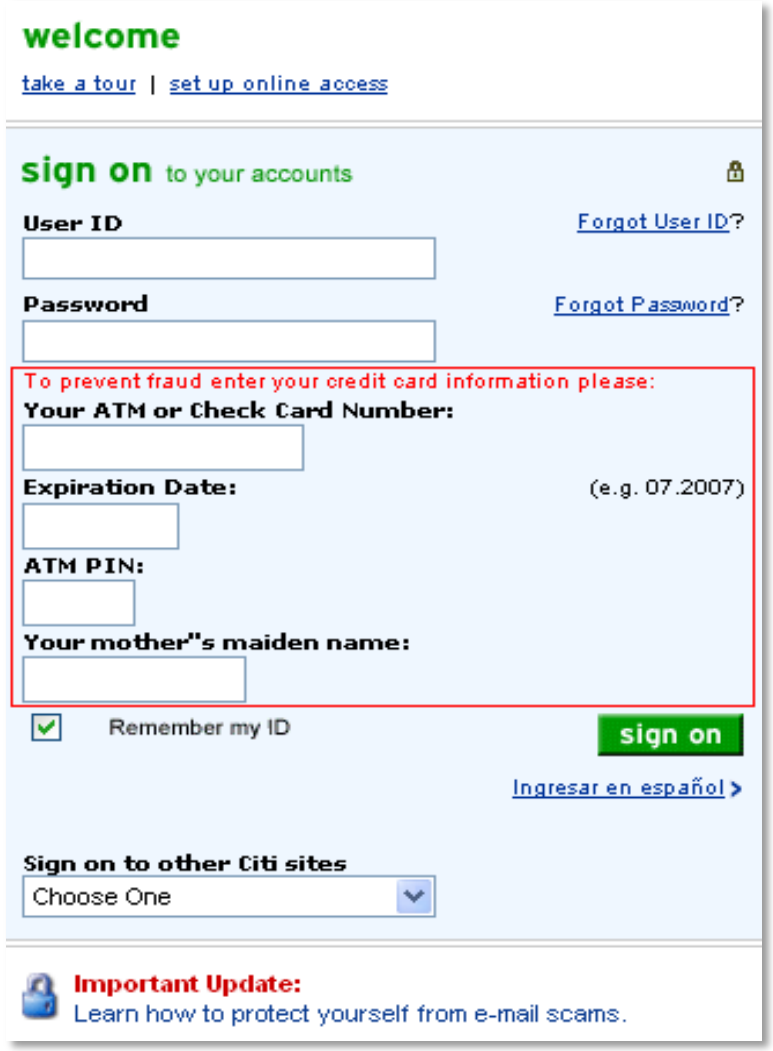
1. **Threats**: Hacking and malware are the major causes
2. **Attacks**: SQLi and HTTP injection for uploading scripts for remote server commands (also increased of 50% from 2010)
3. **Likelihood**: 90% of organizations had at least one data breach over the period of 12 months
4. **Targets**: 54% of incidents target web applications
5. **Data Lost**: Log in credentials, emails and personal identifiable information are the major data types
6. **Business Impact**: The average cost of data breach is estimated as $ 222 per record
7. **Incident Response**: Majority of incidents is discovered after weeks/months from the time of initial data compromise

Sources:

OSF, DataLossDb.org http://www.datalossdb.org
Ponemon Institute and Juniper Research, June 2011 Perceptions about network security,
Ponemon Institute and Symantec, Research March 2012 2011 Cost of a Data Breach: United States
Verizon's Investigative data Breach Report 2012 Verizon Investigative data breach report,

Man in the Browser Attacks





Examples of Malware & Hacking Attacks Used for Online Fraud

- **Account takeover:** hijack web session to take over the victim' s bank account and conduct unauthorized transfer of money from the victim account to a bank account outside the bank
- **Money laundering:** transferring money from illegal proceeds (e.g. sale of drugs) into hacked banking accounts
- **Application fraud:** using stolen credit card and bank account information for opening bank accounts to steal information from the victim and to make payments
- **Card non present fraud:** conducting online purchases with stolen credit card and cardholder data
- **Card counterfeiting:** use of credit and debit card data stolen online to counterfeit card and conduct fraud with ATM/ABM, POS channels
- **Carding:** validation of stolen or purchased debit/credit card data such as CCN, PINs, DOBs, ACC# by using online web forms
- **Identity theft** theft of personal data by phishing/social engineering the victim, using malware (e.g. MitB, keyloggers) as well as by log in into the victim's online banking account

New Technologies Bring New Threats & Attacks

Yesterday

Today

PART II

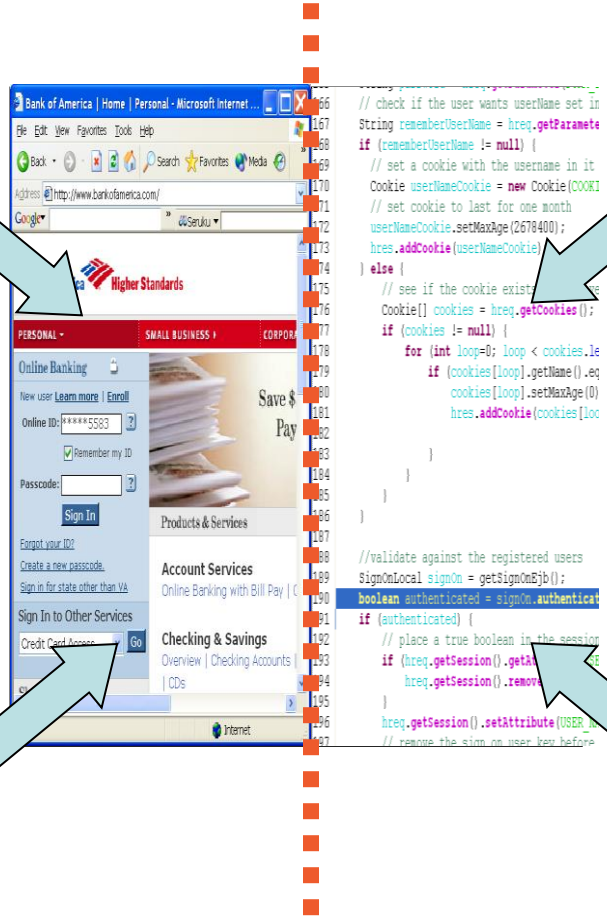
How to adapt application security measures, activities and security tools to protect web applications from hacking and malware threats

"To improve is to change; to be perfect is to change often"
Winston Churchill

Mitigation of Application Vulnerabilities

Manual Penetration Testing

Manual Code Review



Automated Vulnerability Scanning

Automated Static Code Analysis

Mitigating Hacking and Malware Attacks Against Financial Sites

- **Client PC and browser based security measures:**
  - **Awareness of social engineering:** alerts and pointed information for customers on phishing and malware threats
  - **Secure Browser and PC:** keep O.S. and browsers up to date, anti-malware, PC used for online banking with no email, facebook
- **Web application security measures:**
  - **Fixing web application vulnerabilities:** SQL injection, XSS, invalidated redirection, remote command invocations, session management and the rest of OWASP TOP ten vulnerabilities
  - **Validating security of transactions/payments**: positive pay, dual verification & authorizations, anomaly and fraud detection
  - **Out of band transaction validation/authentication:** two way notification confirmation via independent mobile/voice channels
  - **Prevention and detection measures:** strong multi-factor authentication, malicious data filtering/white-listing malicious, web traffic monitoring with WAF and SIEM, behavioral fraud detection

PART III:

What the future holds as the cyber threat landscape continues to change: skills, tools and techniques that can support enterprise security strategy

"I do not feel obliged to believe that the same God who has endowed us with sense, reason, and intellect has intended us to forgo their use."

Galileo Galilei

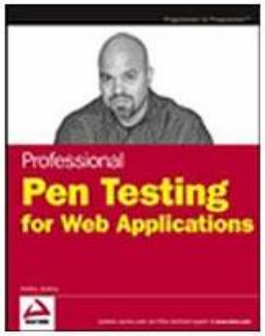
Adapting Application Security Strategy To Hacking and Malware Threats

- **People** trained/hired to conduct threat modeling, design secure applications, build secure software and conduct security testing
- **Processes** for gather threat intelligence analyze threats and vulnerabilities. Risk frameworks for identifying gaps and countermeasures that mitigate malware and hacking risks
- **Technologies** that are effective in protecting and detecting malware attacks, including security tools for testing applications for new vulnerabilities

Application Security Plan For Protecting Applications from Malware and Hacking

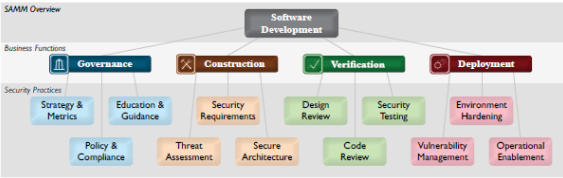
Move on from tactical process

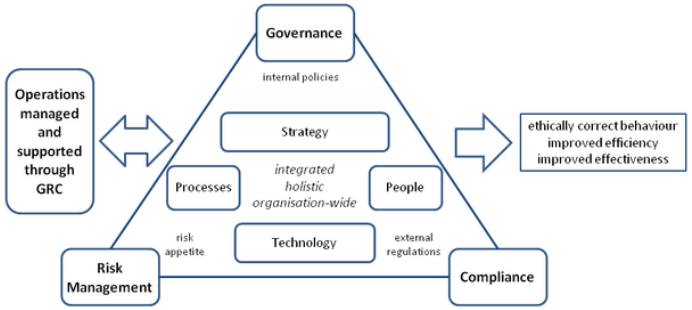
Response to Incidents, Catch and Patch for Vulnerabilities



Invest in strategic security activities

Secure Software Assurance, Governance, Compliance & Risk Management





QUESTIONS & ANSWERS

OWASP References

- Top Ten Vulnerabilities
  - http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf
- Testing Guide
  - https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf
- Development Guide
  - https://www.owasp.org/index.php/OWASP_Guide_Project
- Application Threat Modeling
  - http://www.owasp.org/index.php/Application_Threat_Modeling
- Open Software Assurance Maturity Model (SAMM)
  - http://www.opensamm.org/
- Enterprise Security API for JAVA
  - http://code.google.com/p/owasp-esapi-java/
- Cheat Sheets
  - https://www.owasp.org/index.php/Cheat_Sheets
- OWASP Live CD and Web Application Security
  - http://appseclive.org/
- Application Security Guide for CISO (in progress)
  - https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs