Safeguarding Corporate Data

Gary Johnson, CISSP, CISA

Director, Cyber Solution Engineering and Services

ISM

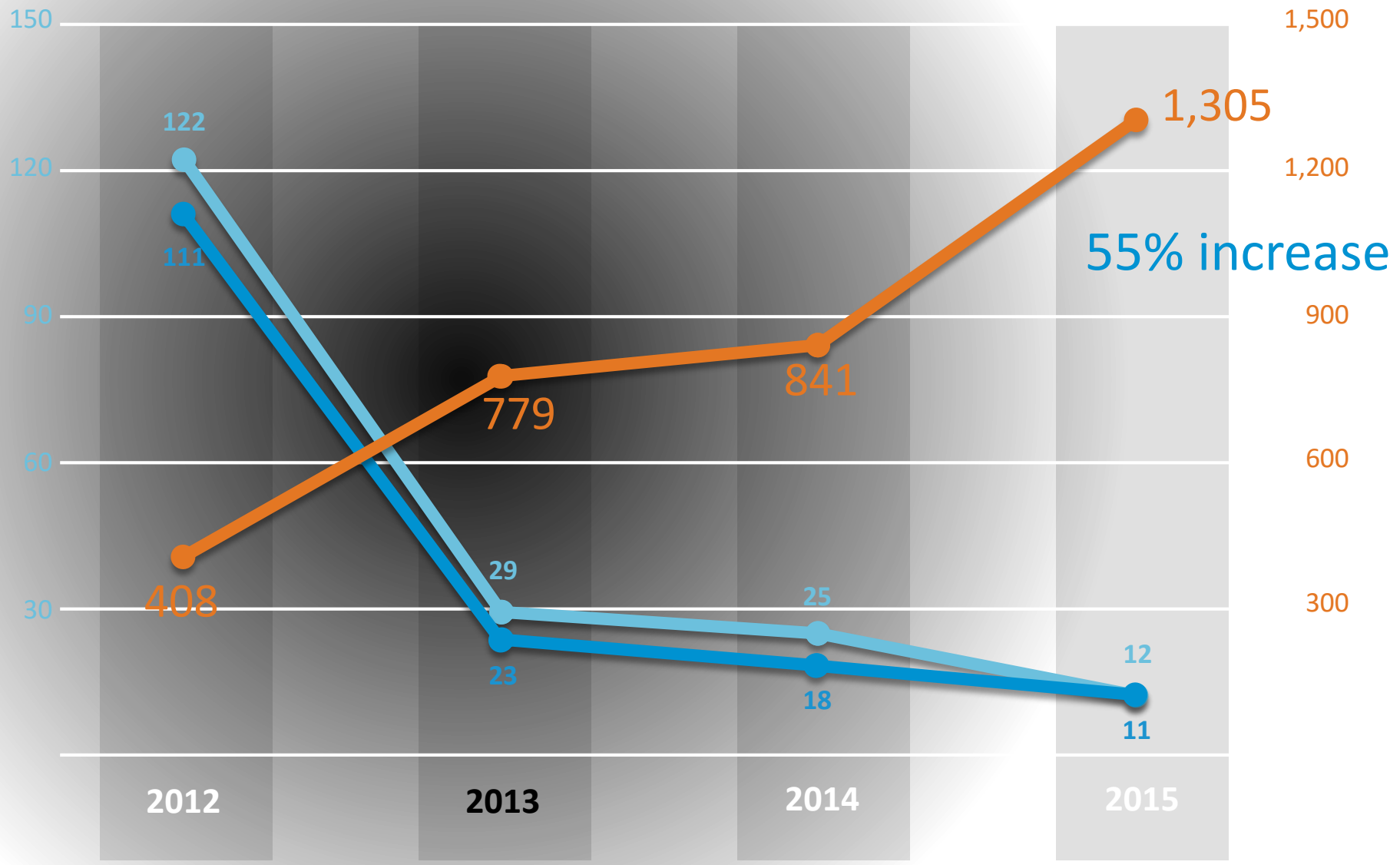
Agenda

- Threat Landscape
- Enterprise Data Protection
- The Problems We Face
- A Multi-layered Approach

Targeted Attacks

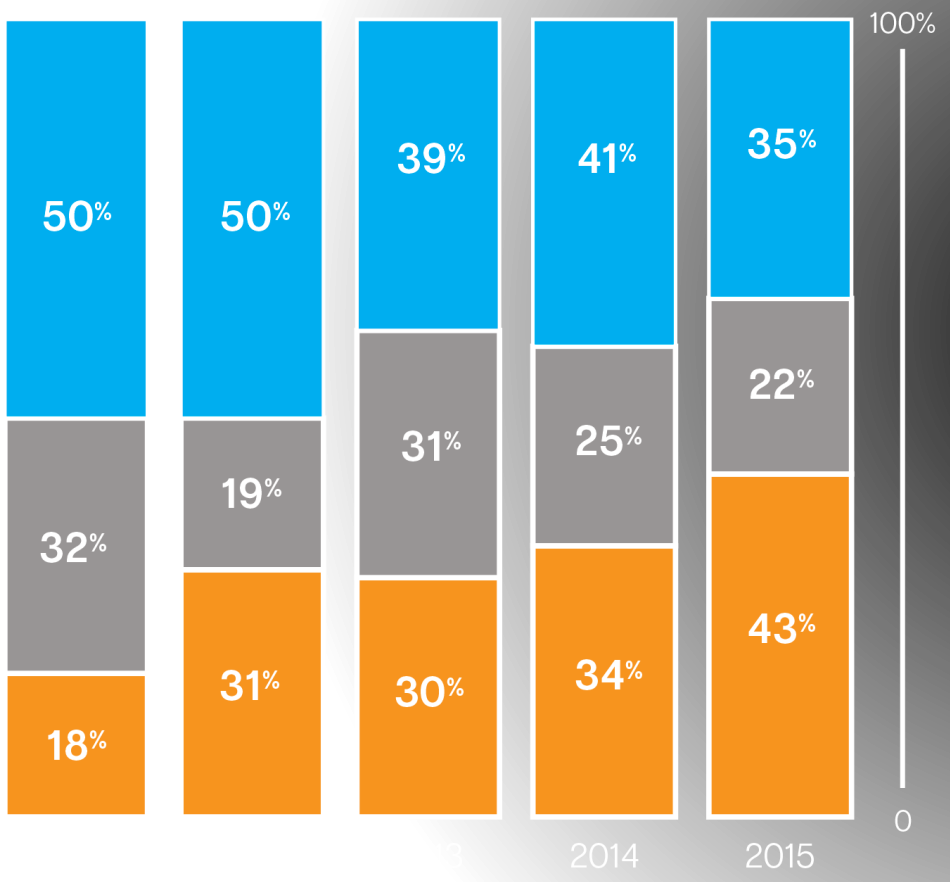
Targeted Attack Campaigns

- Average Number of Email Attacks Per Campaign
- Recipients per Campaign
- Campaigns



Source: Symantec's 2016 Internet Security Threat Report Volume 21

Spear-Phishing Attacks by Size of Targeted Organization

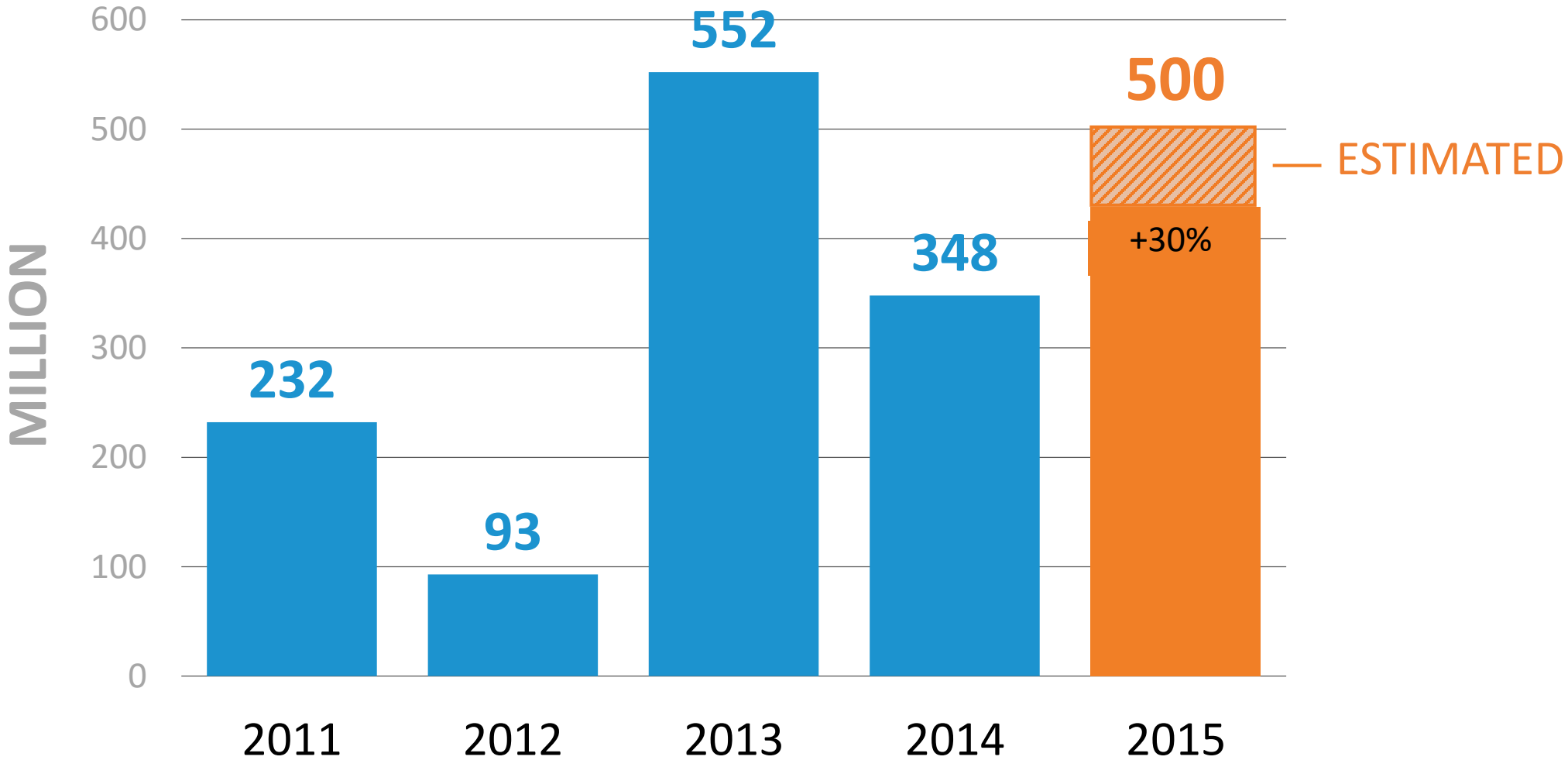


Org Size	2015 Risk Ratio	2015 Risk Ratio as Percentage	Attacks per Org
Large Enterprises **2,500+** Employees	1 in 2.7	38%	3.6
Medium Business **251–2,500** Employees	1 in 6.8	15%	2.2
Small Business (SMB) **1–250** Employees	1 in 40.5	3%	2.1

Source: Symantec's 2016 Internet Security Threat Report Volume 21

Data Breaches

Total Identities Exposed



Source: Symantec 2016 Internet Security Threat Report Volume 21

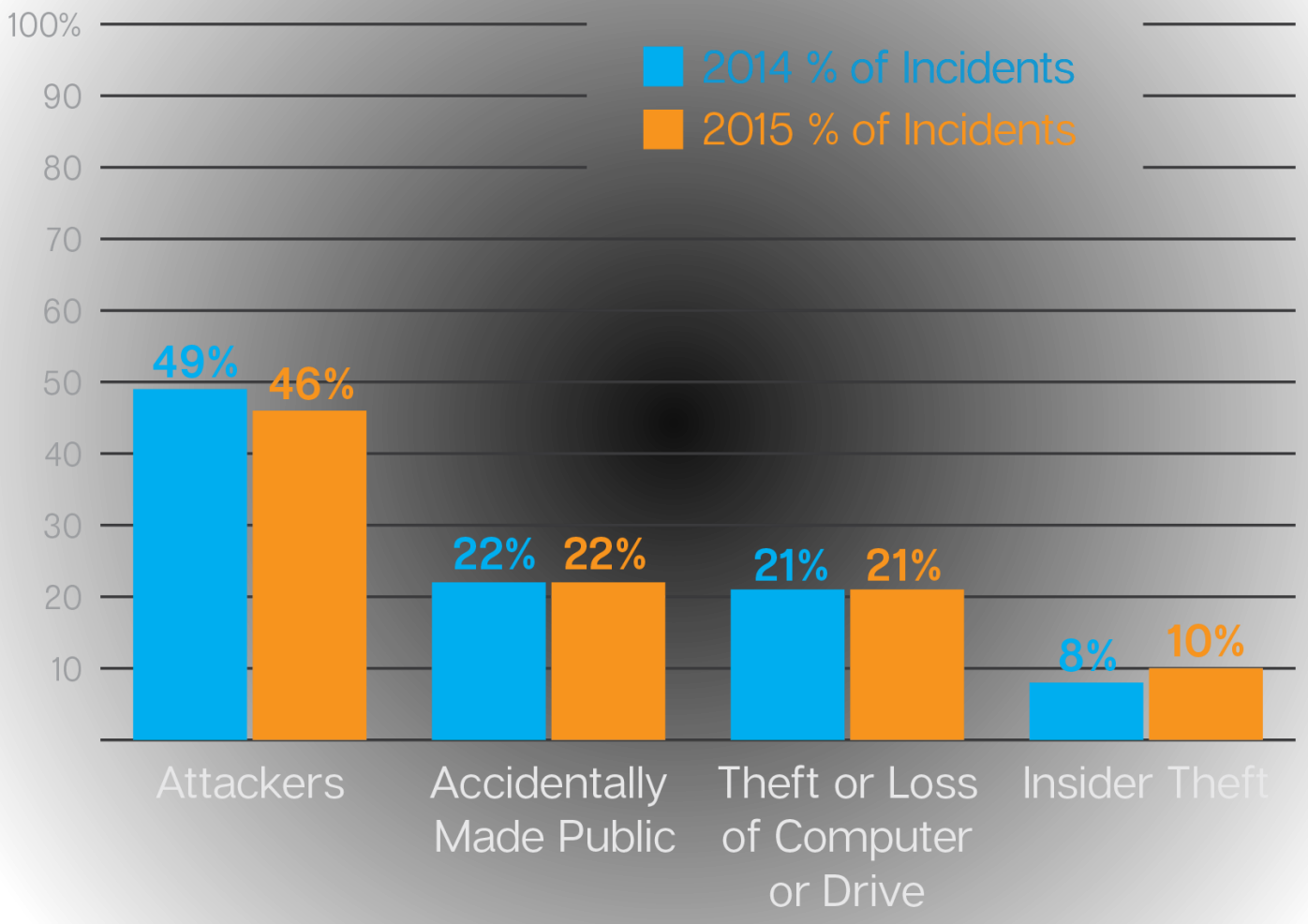
Mega Breaches 2015

Source: Symantec 2016 Internet Security Threat Report Volume 21

> ***"Vendor as a Vector: 97% of breaches featuring stolen credentials leveraged legitimate partner access."***
>
> 2016 Verizon Data Breach Investigations Report

> ***"89% of data breaches had financial gain or espionage motive"***
>
> 2016 Verizon Data Breach Investigations Report

Top Causes of Data Breach by Incidents



Source: Symantec 2016 Internet Security Threat Report Volume 21

Enterprise Data Protection

Enterprise Data Protection

- Data protection is the process of safeguarding important information from corruption and/or loss.
- Data Protection is not just a DLP Solution.
- An enterprise data protection strategy encompasses people, policy, processes, and procedure.
- Best Practice approaches adapted to your organizational needs, requirements, and risk tolerance.
- Protecting an Enterprise requires everyone enabled and working together.
- It’s not just an insider threat issue.

Enterprise Data Protection: The Problem We Face

- Humans are still our weakest link!!!
- The complexities we face are growing as technology continually evolves.
- Budget and resource constraints
- Cloud adoption
- Shadow IT
- Increasing threat from nation states and sophisticated, well funded groups.
- Employee trust can still open organizations up to insider threat

A Multi-layered Approach

Thoughts on a Multi-Layered Approach

"No locale, industry or organization is bulletproof when it comes to the compromise of data."

- 2016 Verizon Data Breach Investigations Report

"The NIST Cybersecurity Framework can be utilized to implement an insider threat mitigation program."

- The SANS Institute

"Insider attacks can be prevented only through a layered defense strategy consisting of policies, procedures, and technical controls."

- CERT, Common Sense Guide to Mitigating Insider Threats

"It is more critical to focus on all aspects of your security posture (people, processes, and technology) than ever before."

- FireEye M-Trends 2016

Multi-layered Approach

- Humans are still our weakest link!!! Security awareness training (that includes Phishing awareness) is essential!
- A comprehensive multi-layered approach will include people, policy, process, procedures, and technology.
- Work to mature you cybersecurity program and practice. Frameworks, standards, and best practices can be helpful in this process.
- Data Protection programs should protect against both insider and outsider threats.
- Know your enemies and know yourself.

Multi-layered Approach

- Mature your asset management and patching process.
- Understand where your data resides and who has access to it. Put controls in place to monitor and protect that data.
- Implement a risk management strategy to identify threats, protect against known threats, detect unknown threats, increase your ability to respond to and contain attacks when they happen, and recover from attacks/compromise.
- Leverage rich security intelligence and advanced tools to identify indicators of compromise.
- Leverage lessons learned and other data driven metrics to continually improve and mature your enterprise data protection program.

Thank You!

Gary Johnson, CISSP, CISA
Director, Cyber Solution Engineering and Services
ISM
gjohnson@ism.com
Office: 301-670-1813 Ext 124