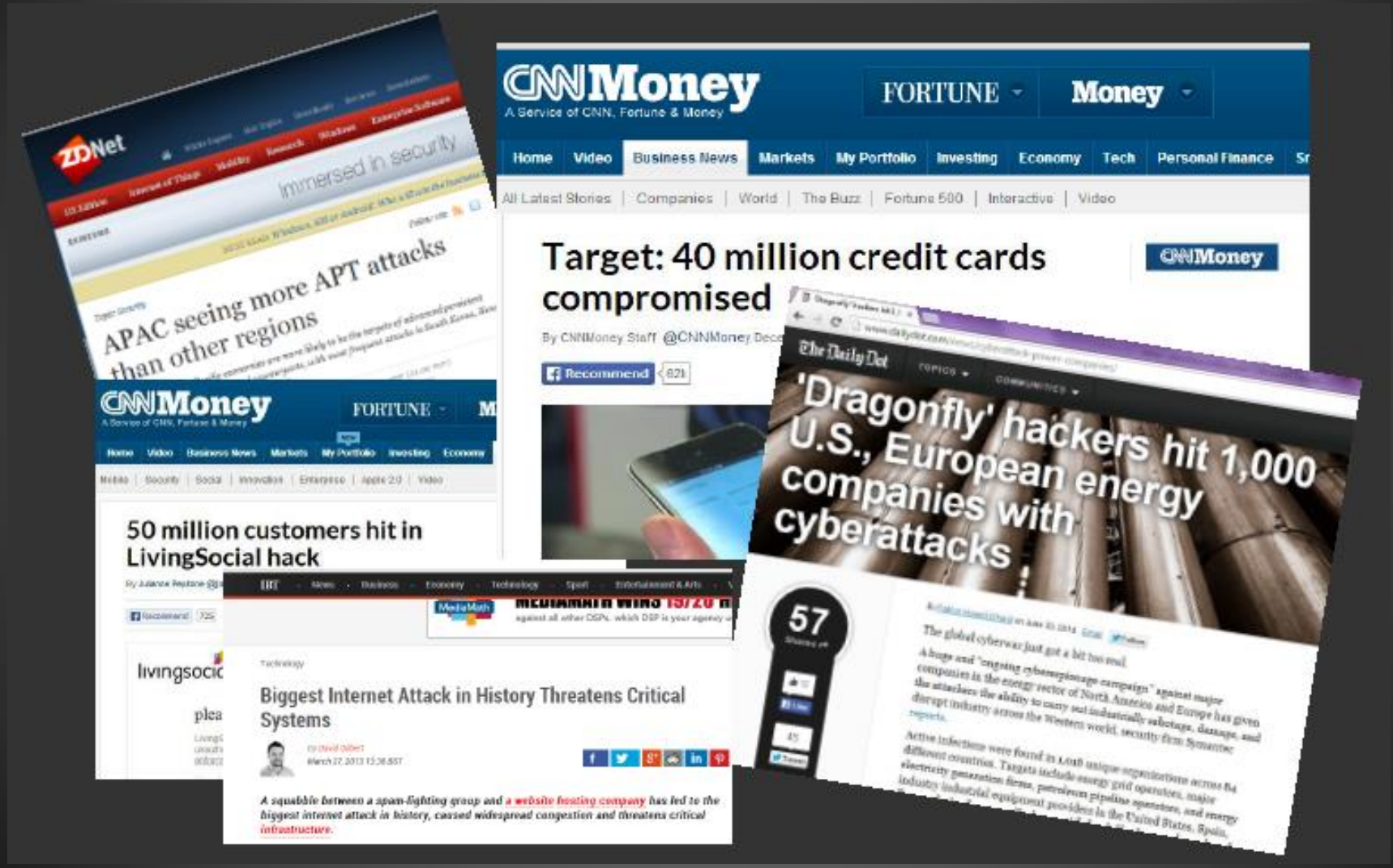
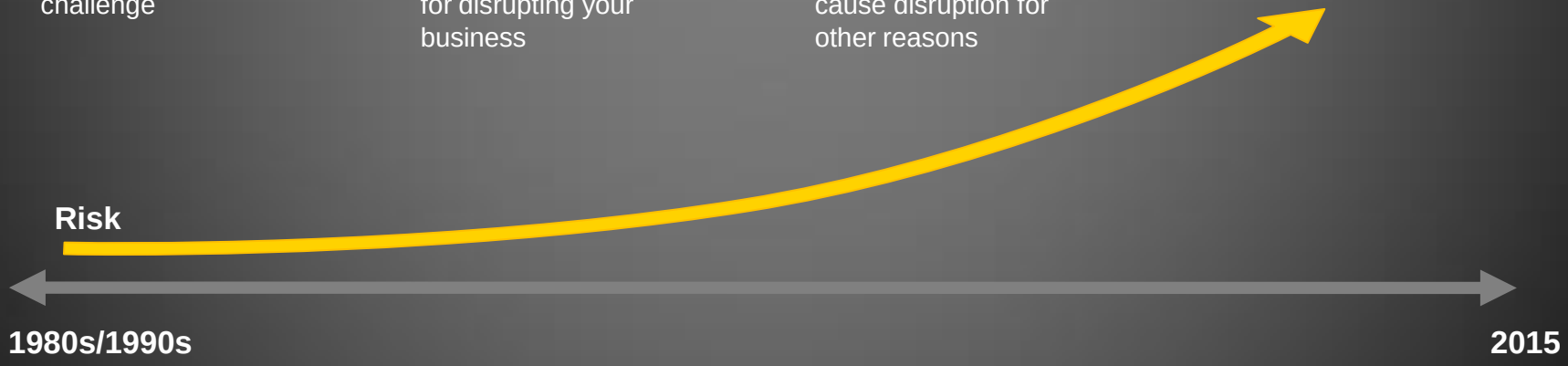

GSW Session:
Protecting Your Business
in the Internet Age
May 2015
Sergio Kogan
EY Partner - Cybersecurity
EY
Building a better
working world

Cyber attacks are headline news

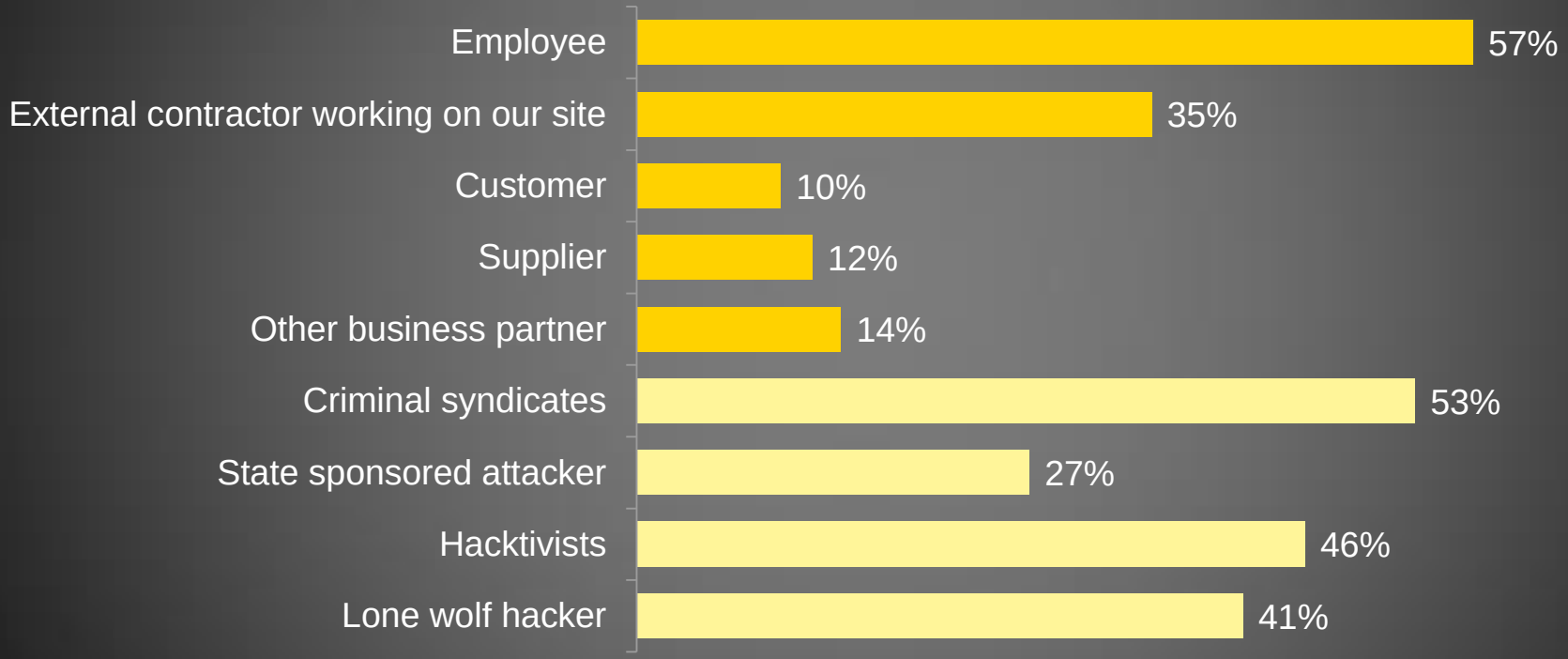


Evolution of threats – attacks become better funded and more sophisticated every year

Unsophisticated attackers (script kiddies)	Sophisticated attackers (hackers)	Corporate espionage (malicious insiders)	State sponsored attacks Advanced Persistent Threat (APT)
► You are attacked because you are on the internet and have a vulnerability – you represent a challenge	► You are attacked because you are on the internet and have information of value – or they have a reason for disrupting your business	► Your current or former employee seeks financial gain from stealing/selling your IP – or they want to cause disruption for other reasons	► You are targeted because of who you are, what you do, or the value of your intellectual property

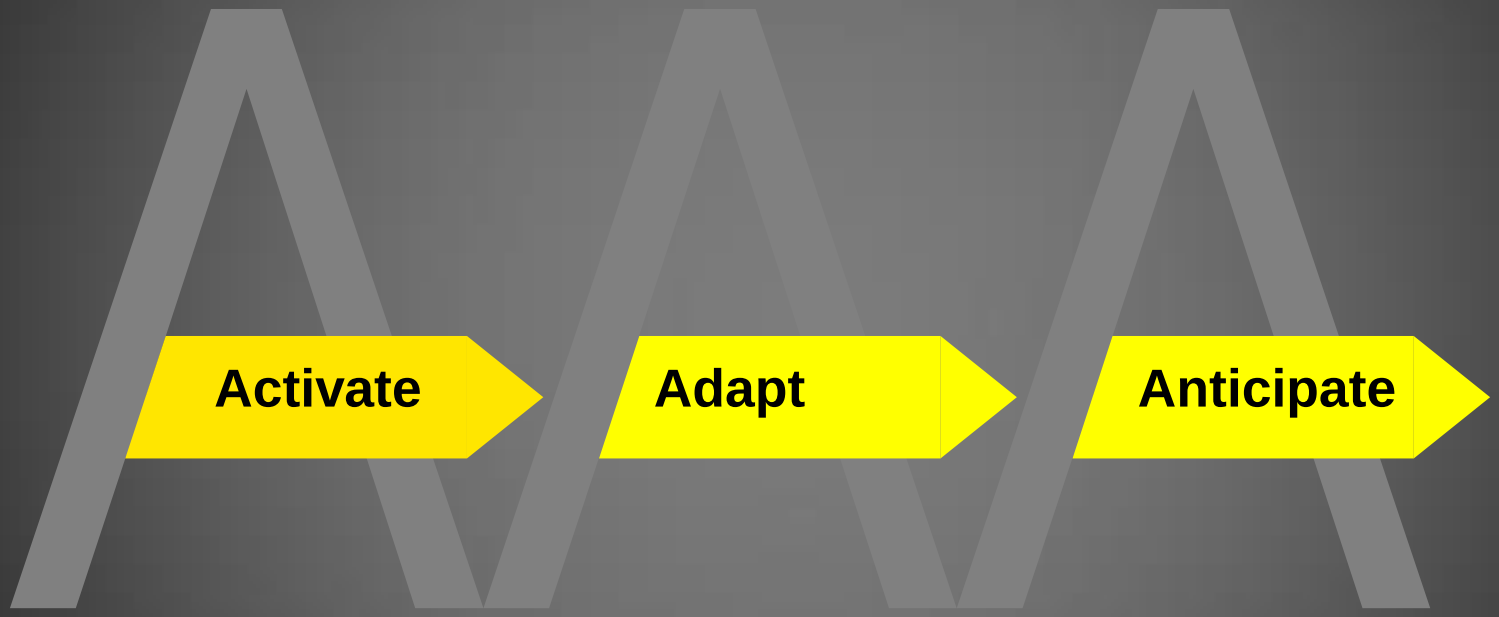


Who or what do you consider the most likely source of an attack?”



EY Global Information Security Survey 2014.

Protecting Your Business in the Internet Age
Focus on the three As



A 3-stage improvement process

To protect your business in the internet age we suggest that organizations adopt a 3-stage improvement process:

1. Activate (a foundational approach)

   Organizations need to establish and improve the solid foundations of their cybersecurity)

2. Adapt (a dynamic approach)

   Because organizations are constantly changing and cyber threats are evolving, cybersecurity needs to be able to adapt to changing requirements

3. Anticipate (a proactive approach)

   Organizations need to make efforts to predict what is coming so they can be better prepared for the inevitable cyber attacks)

Appendix

Foundational activities all organizations need to “activate”

1. Conduct a cyber threat assessment and design an implementation roadmap
2. Get Board-level support for a security transformation
3. Review and update security policies, procedures and supporting standards
   - Implement an information security management system
4. Establish a Security Operations Center (SOC)
   - Develop monitoring and incident response procedures
5. Design and implement cybersecurity controls
   - Assess the effectiveness of data loss prevention and identity and access management processes
   - Harden the security of IT assets
6. Test business continuity plans and incident response procedures

Adapt – take action to improve and transform

1. Design and implement a transformation program
   - Get external help in designing the program, and providing program management
2. Decide what to keep in-house and what to outsource
3. Define a RACI matrix for cybersecurity
4. Define the organization's ecosystem
   - Make moves to eliminate or lessen potential security gaps in your interaction with third parties
5. Introduce cybersecurity awareness training for employees

Anticipate Take action – and get ahead

1. Design and implement a cyber threat intelligence strategy
   - Use threat intelligence to support strategic business decisions
2. Define and encompass the organization's extended cybersecurity ecosystem
   - Define RACI and trust models and enact cooperation, sharing capabilities where advantageous
3. Take a cyber economic approach
   - Understand the value of your most vital cyber assets
4. Use forensics and analytics
   - Use the latest technical tools to analyze where the likely threats are coming from and when
5. Ensure everyone understands what's happening
   - Strong governance, user controls and regular communications