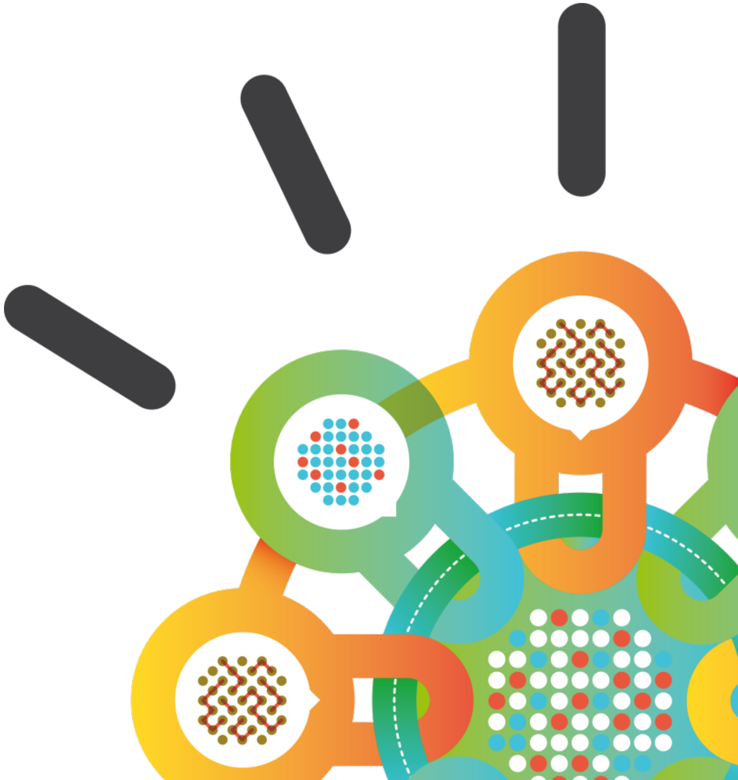
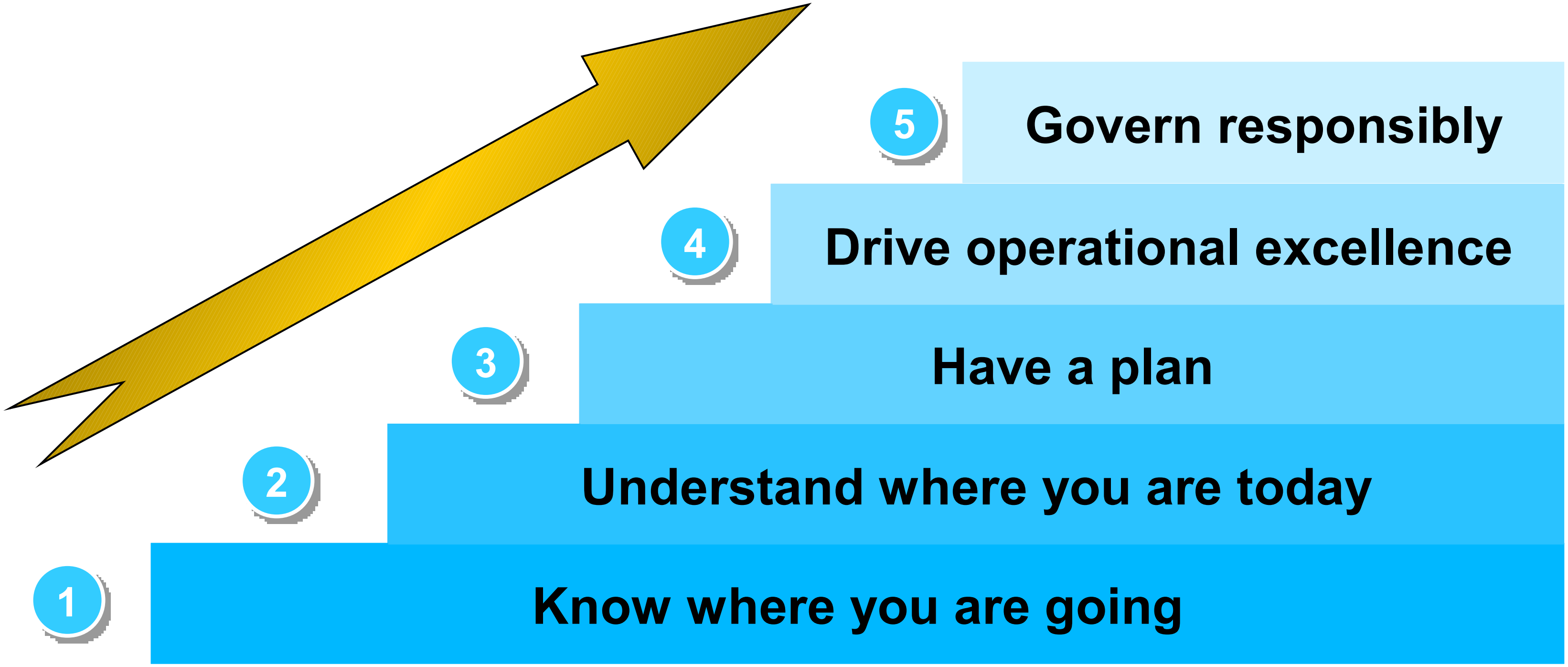
Security Intelligence.
Think Integrated.

Five Key Steps to Success in Application Security



How our successful clients have developed their application security programs



1 Know where you are going

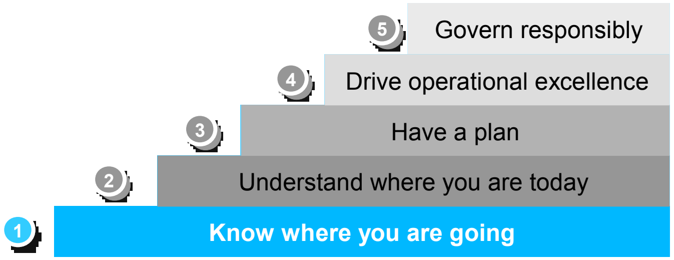
2 Understand where you are today

3 Have a plan

4 Drive operational excellence

5 Govern responsibly

Step 1: Know where you are going



5 Govern responsibly

4 Drive operational excellence

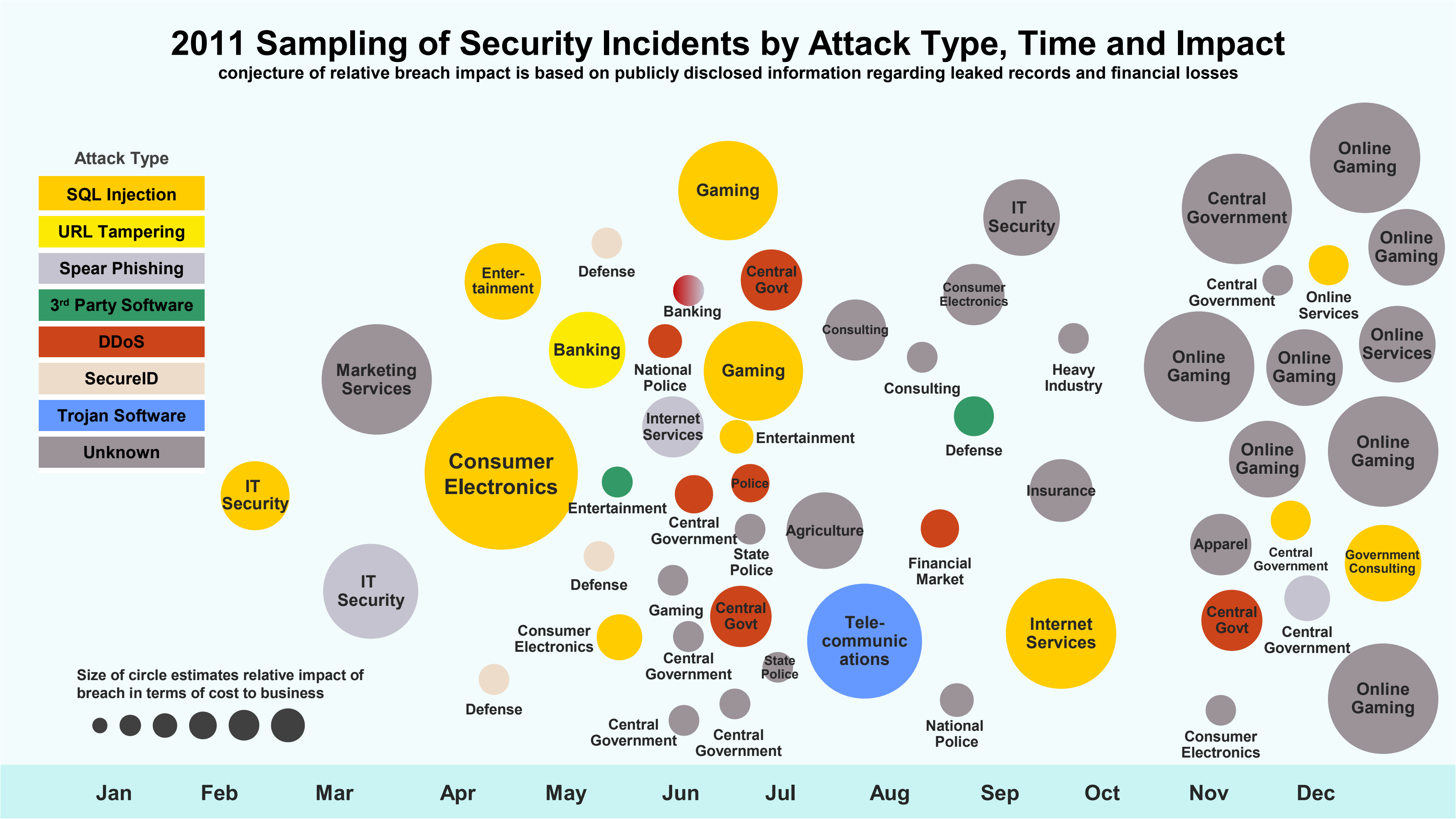
3 Have a plan

2 Understand where you are today

1 **Know where you are going**

- Understand the problem
  - The security landscape
- Understand the risks
  - What makes sense for your industry
  - Comparable companies and breaches
- Understand the rules
  - Compliance requirements that you have to meet

Data breaches come in all shapes and sizes



2011 Sampling of Security Incidents by Attack Type, Time and Impact

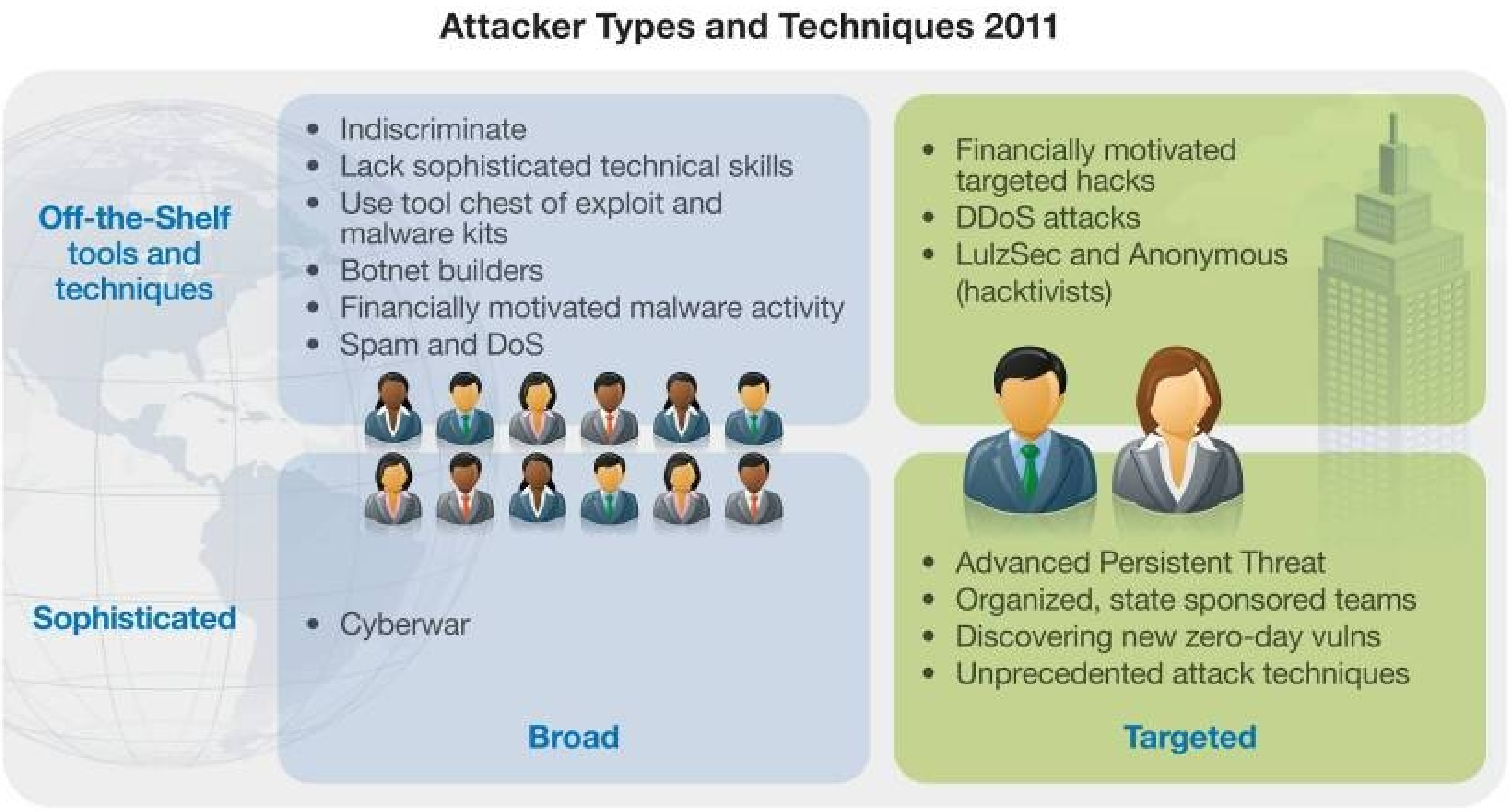
conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Size of circle estimates relative impact of breach in terms of cost to business

Source: IBM X-Force® Research 2011 Trend and Risk Report

JK 2012-04-26

Attackers have a variety of motivations



Attacker Types and Techniques 2011

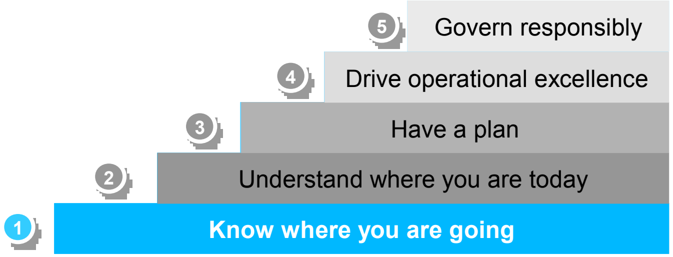
	Broad	Targeted
Off-the-Shelf tools and techniques	• Indiscriminate • Lack sophisticated technical skills • Use tool chest of exploit and malware kits • Botnet builders • Financially motivated malware activity • Spam and DoS	• Financially motivated targeted hacks • DDoS attacks • LulzSec and Anonymous (hacktivists)
Sophisticated	• Cyberwar	• Advanced Persistent Threat • Organized, state sponsored teams • Discovering new zero-day vulns • Unprecedented attack techniques

Source: IBM X-Force® Research and Development

A sampling of compliance regulations with security impact

Regulation	Who it affects
Payment Card Industry (PCI-DSS)	All merchants, banks, and service providers that store, process, or transmit cardholder data must comply with the PCI Data Security Standard
Health Insurance Portability and Accountability Act (HIPAA)	All entities that handle maintain, store, or exchange private health or patient-related information, regardless of size This includes the following: healthcare organizations; employers maintaining health records; health plans; life insurers; most doctors, nurses, pharmacies, hospitals, clinics, nursing homes
Data Protection Act 1998 (DPA)	Any business that processes personal information in the UK
Sarbanes-Oxley Act (SOX)	All corporations that fall under the jurisdiction of the U.S. Securities and Exchange Commission (essentially any publicly traded company in the US
<and many more>	

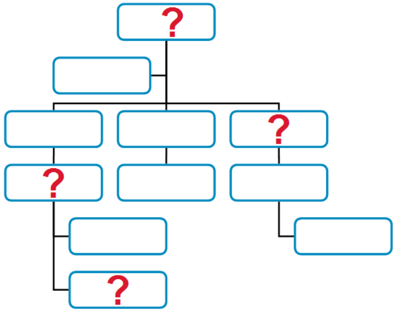
Step 1: *“Know where you are going”*
Things you can do


5 Govern responsibly
4 Drive operational excellence
3 Have a plan
2 Understand where you are today
1 Know where you are going

Gather this essential data

1. Educate yourself

2. Answer: Who cares?...

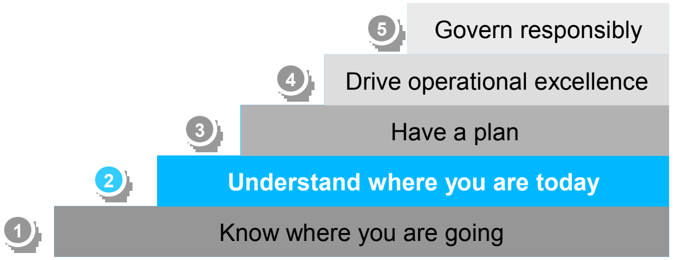


3. …How much?...

4. …How soon?

5. Find a sponsor

Step 2: Understand where you are today



5 Govern responsibly

4 Drive operational excellence

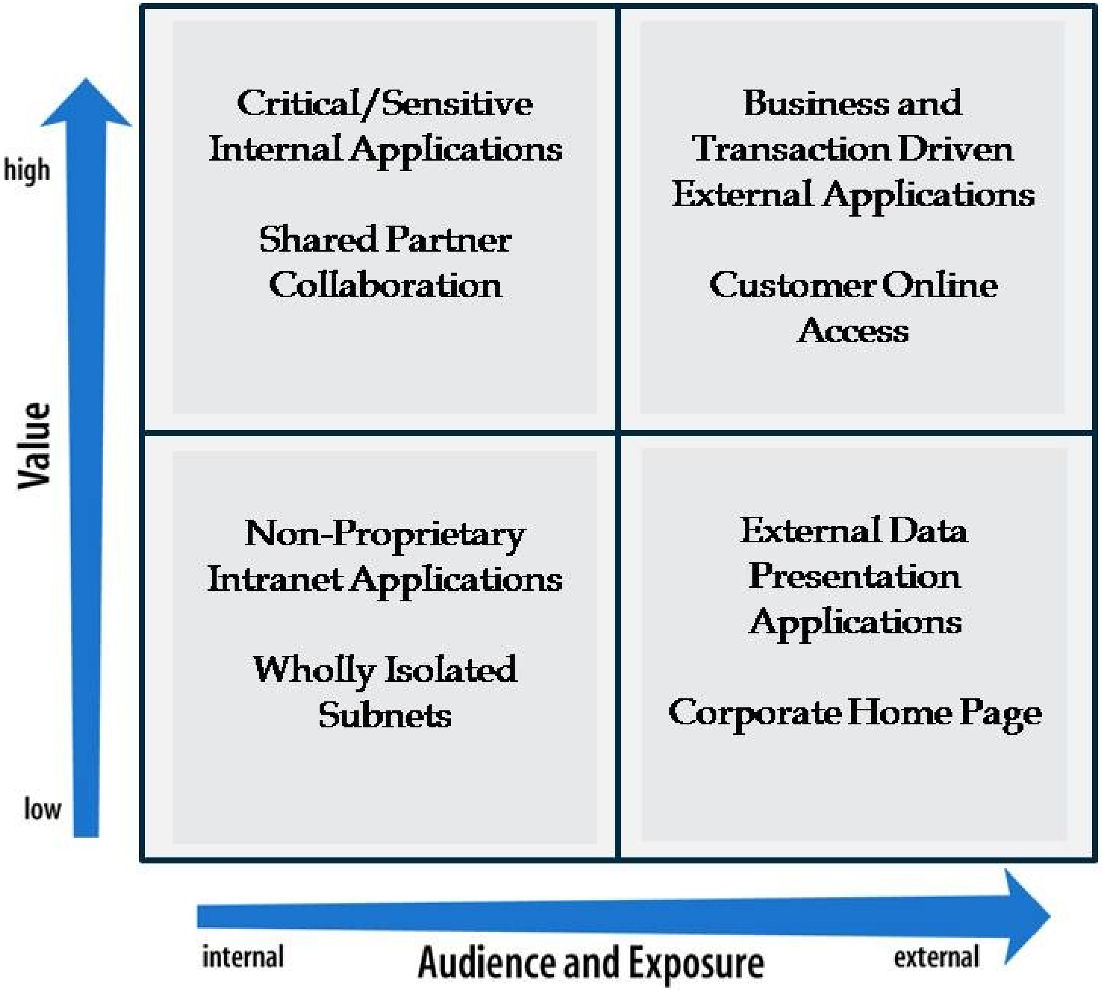
3 Have a plan

2 **Understand where you are today**

1 Know where you are going

- Understand what you have
- Prioritize the risk level
- Take a snapshot of vulnerabilities

When it comes to risk, all applications are not created equal



Critical/Sensitive Internal Applications

Shared Partner Collaboration

Business and Transaction Driven External Applications

Customer Online Access

Non-Proprietary Intranet Applications

Wholly Isolated Subnets

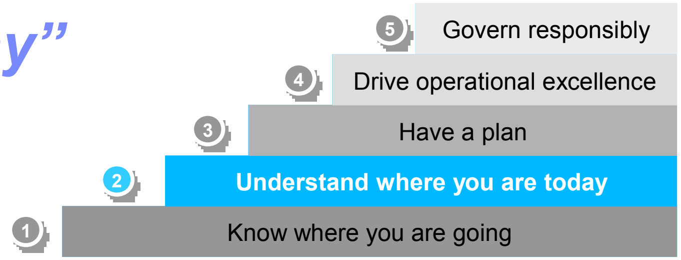
External Data Presentation Applications

Corporate Home Page

Initial vulnerability assessment can help you assess where you are today

- How to get started
  - Pick one or two applications
    - Receptiveness of the stakeholders and development teams is a key factor
    - Initial applications should be important to the business
    - Note that your most critical applications may already be your most secure
  - Perform a vulnerability assessment
  - Perform a risk/threat analysis
- Use this experience as an indicator of what your program needs to be

Step 2: *"Understand where you are today"* Things you can do


5 Govern responsibly

4 Drive operational excellence

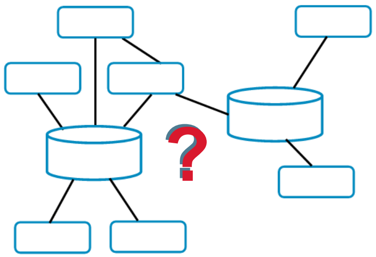
3 Have a plan

2 Understand where you are today

1 Know where you are going

Assess your application security risk level

1. What have you got?



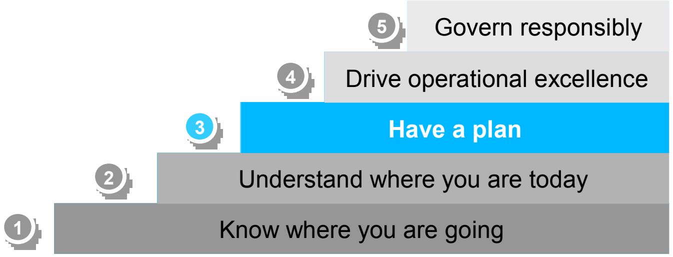
2. Who owns it?

3. Who can access it?

4. What's the risk?

5. Update your sponsor

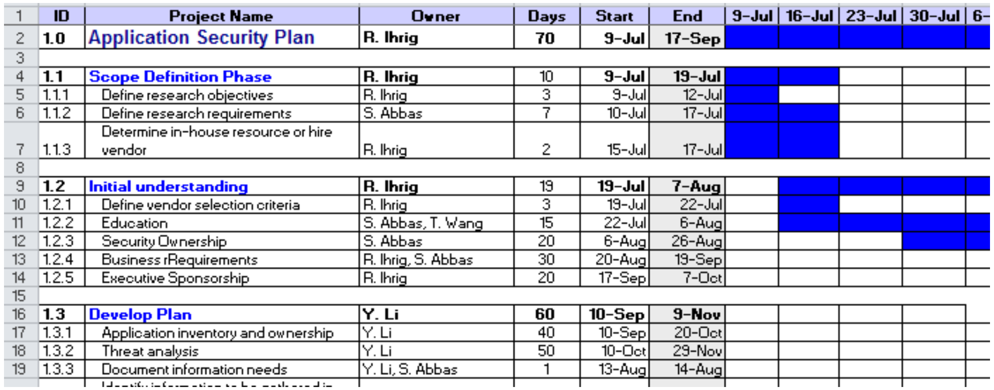
Step 3: Have a plan


5 Govern responsibly
4 Drive operational excellence
3 Have a plan
2 Understand where you are today
1 Know where you are going

- You can’t do it all at once, you have to start somewhere

- Build a repeatable process that you can scale to improve coverage

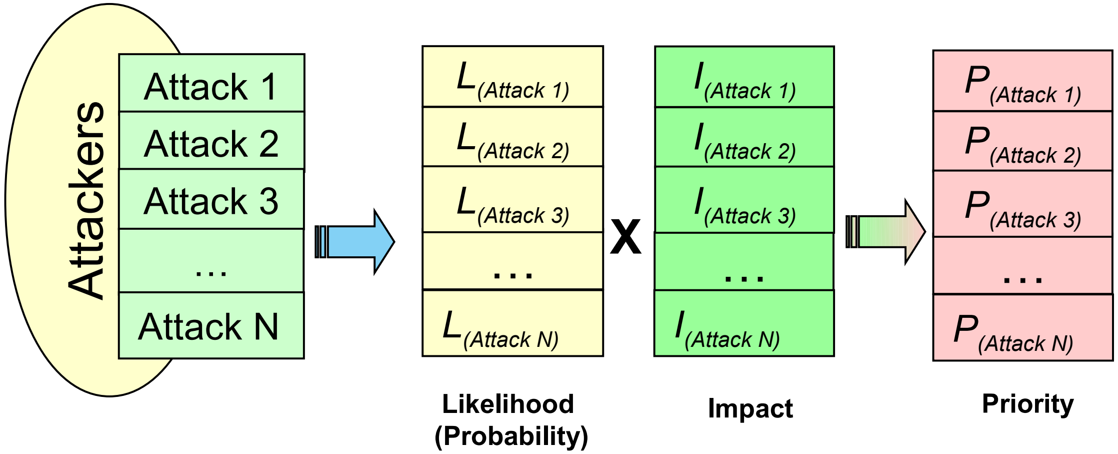
- Use early success to get others in the organization on board



1	ID	Project Name	Owner	Days	Start	End	9-Jul	16-Jul	23-Jul	30-Jul	6-
2	**1.0**	**Application Security Plan**	**R. Ihrig**	**70**	**9-Jul**	**17-Sep**	■	■	■	■	■
3											
4	**1.1**	**Scope Definition Phase**	**R. Ihrig**	10	**9-Jul**	**19-Jul**	■	■			
5	1.1.1	Define research objectives	R. Ihrig	3	9-Jul	12-Jul	■				
6	1.1.2	Define research requirements	S. Abbas	7	10-Jul	17-Jul	■	■			
7	1.1.3	Determine in-house resource or hire vendor	R. Ihrig	2	15-Jul	17-Jul	■	■			
8											
9	**1.2**	**Initial understanding**	**R. Ihrig**	19	**19-Jul**	**7-Aug**		■	■	■	■
10	1.2.1	Define vendor selection criteria	R. Ihrig	3	19-Jul	22-Jul		■			
11	1.2.2	Education	S. Abbas, T. Wang	15	22-Jul	6-Aug		■	■	■	■
12	1.2.3	Security Ownership	S. Abbas	20	6-Aug	26-Aug				■	■
13	1.2.4	Business rRequirements	R. Ihrig, S. Abbas	30	20-Aug	19-Sep					
14	1.2.5	Executive Sponsorship	R. Ihrig	20	17-Sep	7-Oct					
15											
16	**1.3**	**Develop Plan**	**Y. Li**	**60**	**10-Sep**	**9-Nov**					
17	1.3.1	Application inventory and ownership	Y. Li	40	10-Sep	20-Oct					
18	1.3.2	Threat analysis	Y. Li	50	10-Oct	29-Nov					
19	1.3.3	Document information needs	Y. Li, S. Abbas	1	13-Aug	14-Aug					
		Identify information to be gathered in									

Starting your application security program

- Prioritize a small number of applications to work with
  - Based on risk
  - Based on stakeholders



Attackers

Attack 1
Attack 2
Attack 3
…
Attack N

$L_{(Attack\ 1)}$
$L_{(Attack\ 2)}$
$L_{(Attack\ 3)}$
…
$L_{(Attack\ N)}$

X

$I_{(Attack\ 1)}$
$I_{(Attack\ 2)}$
$I_{(Attack\ 3)}$
…
$I_{(Attack\ N)}$

$P_{(Attack\ 1)}$
$P_{(Attack\ 2)}$
$P_{(Attack\ 3)}$
…
$P_{(Attack\ N)}$

Likelihood (Probability)

Impact

Priority

- Plug the critical holes
  - Fixing the defects might not be possible or practical

Fix the application

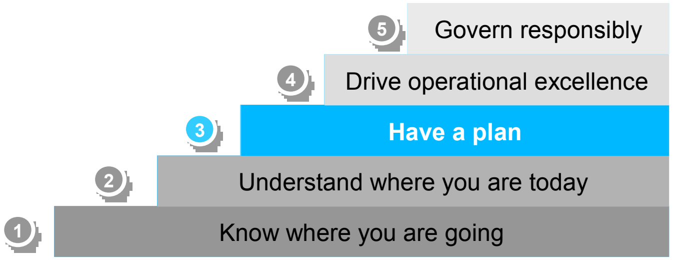
AND/OR

Protect the application

- Enlarge the coverage
  - Develop models for repeatable process and effective roles

PLUS

Step 3: *"Have a plan"*
Things you can do



5 Govern responsibly

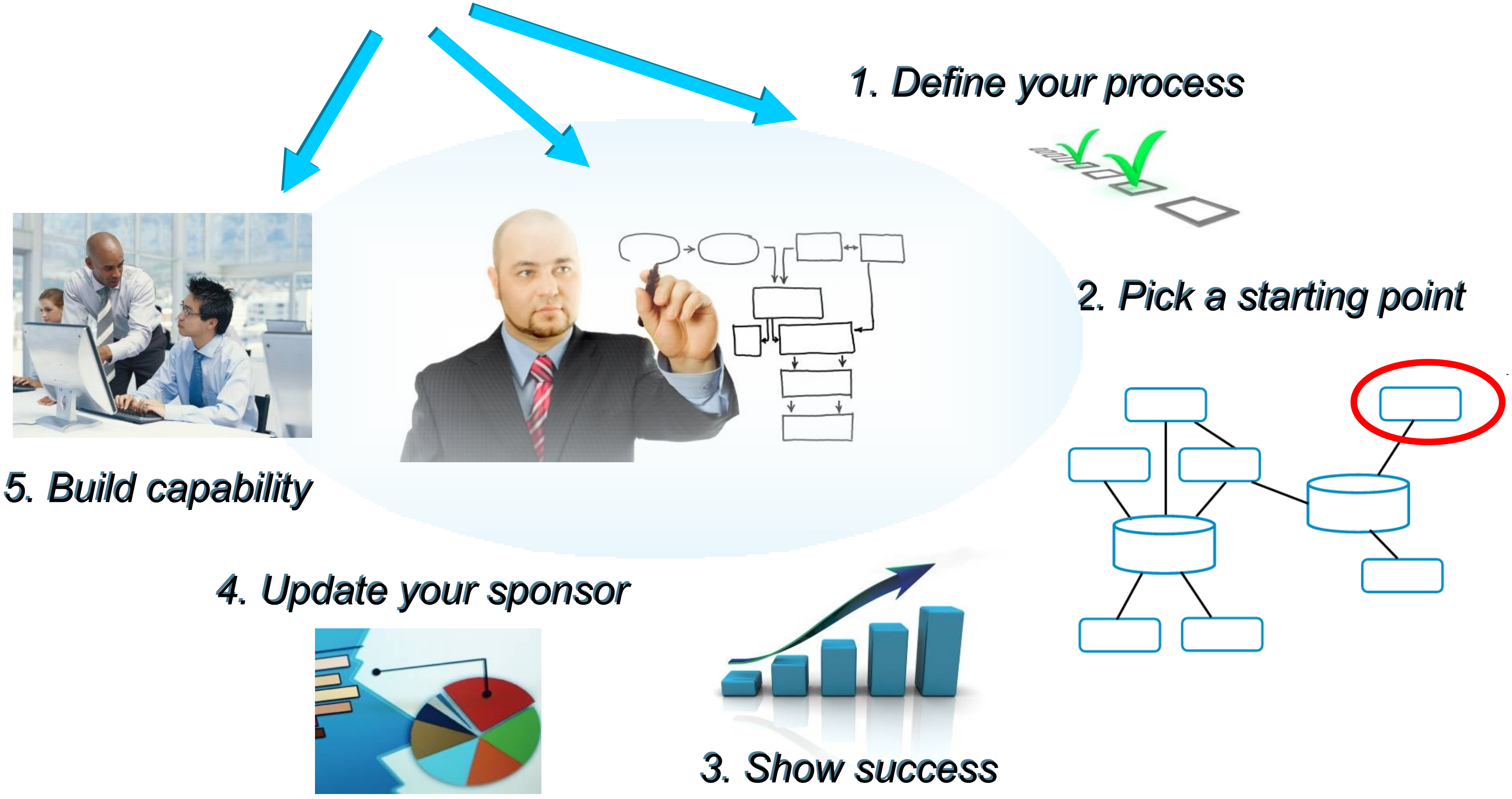
4 Drive operational excellence

3 **Have a plan**

2 Understand where you are today

1 Know where you are going

Take a phased approach



1. Define your process

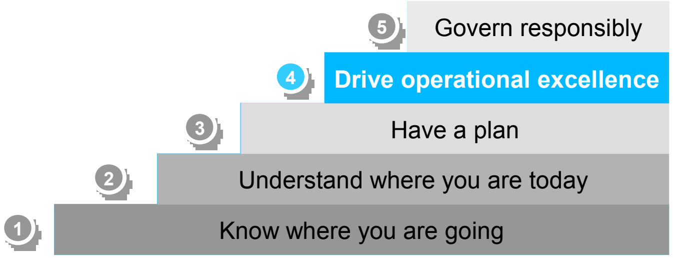
2. Pick a starting point

3. Show success

4. Update your sponsor

5. Build capability

Step 4: Drive Operational Excellence



5 Govern responsibly
4 Drive operational excellence
3 Have a plan
2 Understand where you are today
1 Know where you are going

- Get Security and Development working together
- Build Security In From The Start
- Reduce the Cost of Being Secure

The cultural divide between Security and Development teams

Developers Lack Security Focus

Software functionality ≠Security

Software complexity ≠Security

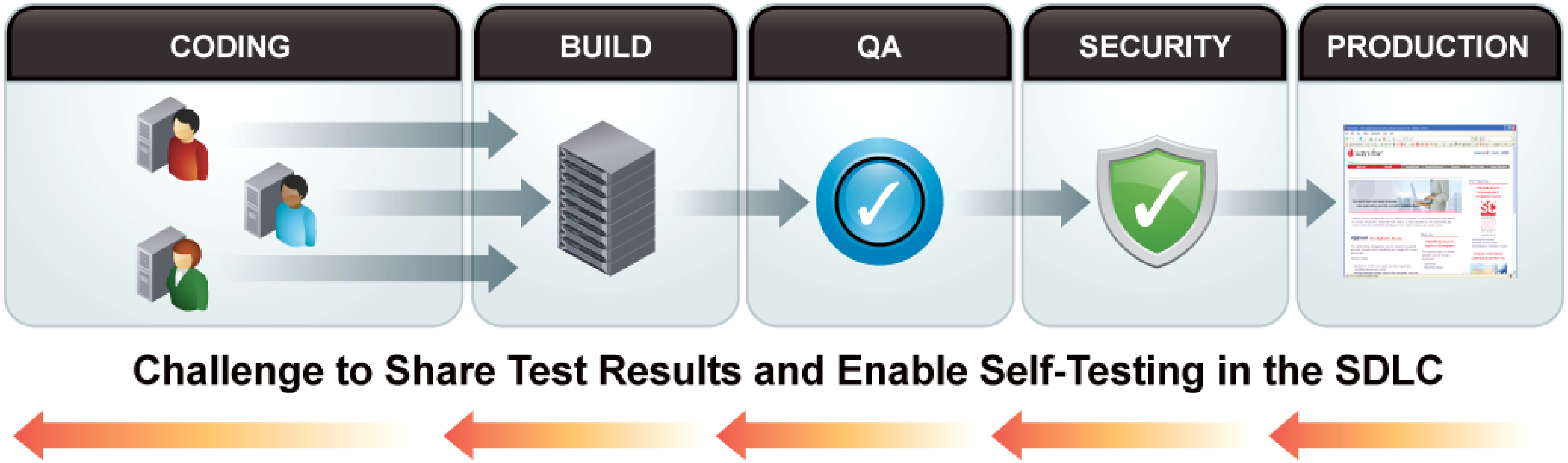
No security requirements = No security

Security Team = SDLC bottleneck

Security priority ≠Development priority

Security showstopper ≠ Development showstopper

Security headcount < Development headcount

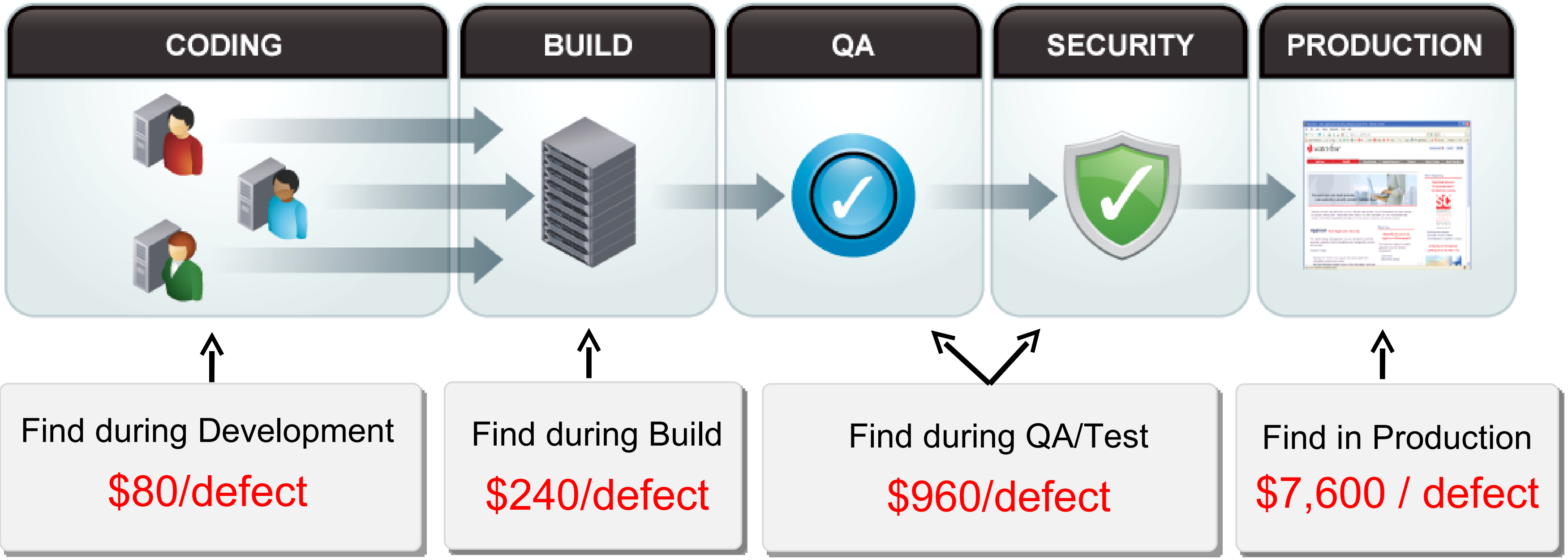


Challenge to Share Test Results and Enable Self-Testing in the SDLC

You can reduce the cost of fixing vulnerabilities by finding them as early as possible in the development cycle

*80% of development costs are spent identifying and correcting defects!**

Average Cost of a Data Breach
$5.5M** from law suits, loss of customer trust, damage to brand



Find during Development
$80/defect

Find during Build
$240/defect

Find during QA/Test
$960/defect

Find in Production
$7,600 / defect

* Source: National Institute of Standards and Technology

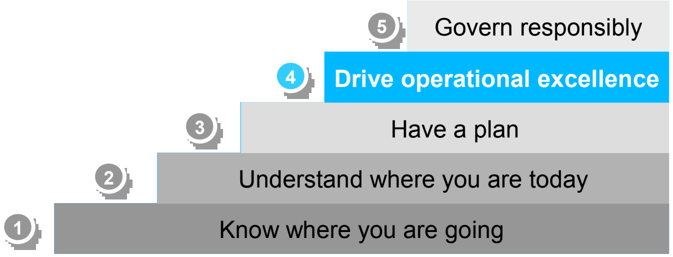
** Source: Ponemon Institute 2011

Increase your organizational maturity – move from *Basic* to *Optimized* over time

Security Intelligence

	People	Data	Applications	Infrastructure
Optimized	**Security Intelligence:** Information and event management Advanced correlation and deep analytics External threat research			
	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Secure systems
Proficient	User provisioning Access management Strong authentication	Database vulnerability monitoring Access monitoring Data loss prevention	Glass box scanning Static analysis	Virtualization security Asset management Endpoint / network security management
Basic	Centralized directory	Encryption Access control	Dynamic analysis	Perimeter security Anti-virus

Step 4: *"Drive Operational Excellence"*
Things you can do



5 Govern responsibly

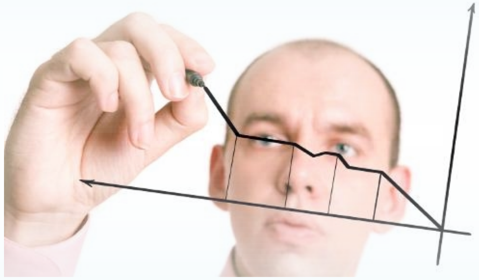
4 Drive operational excellence

3 Have a plan

2 Understand where you are today

1 Know where you are going

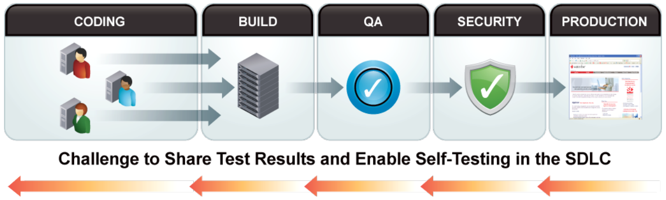
It's about People, Process and Technology



1. Get teams talking

2. Track security repair costs

3. Reduce delays and costs by testing earlier

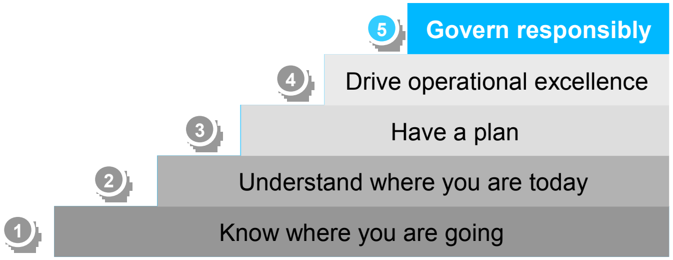


Challenge to Share Test Results and Enable Self-Testing in the SDLC

4. Use automation to reduce effort

5. Report to sponsor on investments and savings

Step 5: Govern Responsibly



5 Govern responsibly

4 Drive operational excellence

3 Have a plan

2 Understand where you are today

1 Know where you are going

- Maintain your security posture
  - Where are you today?
  - Are you better or worse than you were yesterday?
- Keep everyone informed
  - Executives, The Board, Management, Security, Development, QA
- Play by the Rules
  - Governance and tracking are key to meeting your compliance obligations

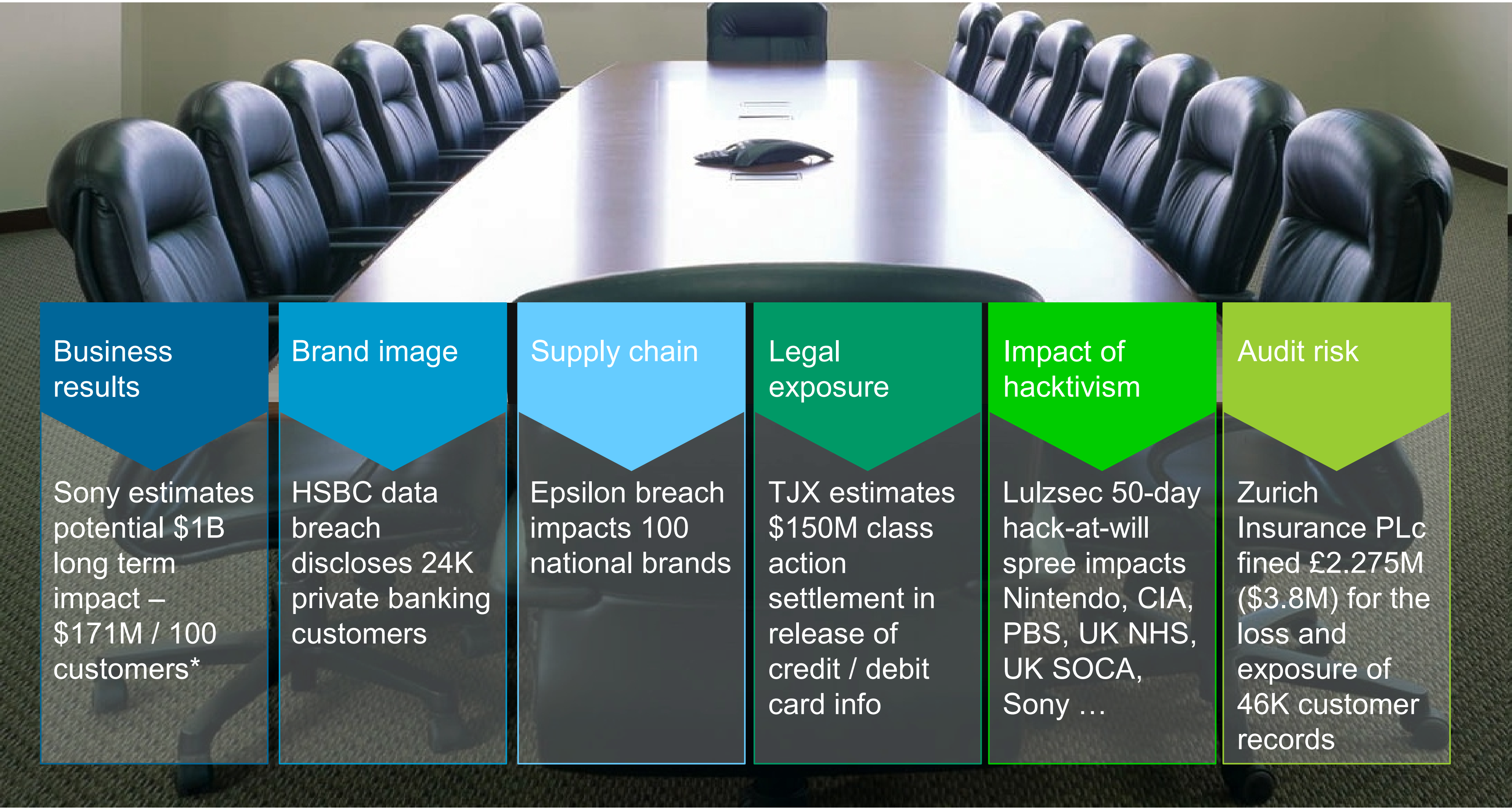
AUDIT REPORT

☑ **Audit satisfactory**
~ verifies compliance with requirements

□ Non-conformances found

□ Observations made

Highly public exploits bring security to the board room



Business results

Sony estimates potential $1B long term impact – $171M / 100 customers*

Brand image

HSBC data breach discloses 24K private banking customers

Supply chain

Epsilon breach impacts 100 national brands

Legal exposure

TJX estimates $150M class action settlement in release of credit / debit card info

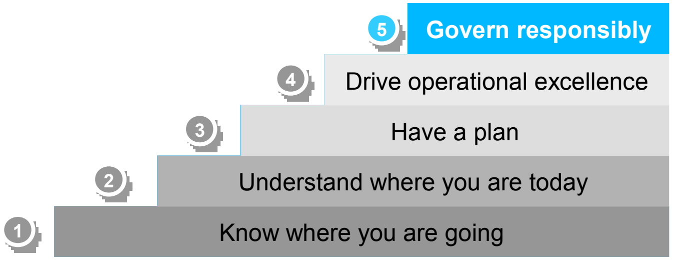
Impact of hacktivism

Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony …

Audit risk

Zurich Insurance PLc fined £2.275M ($3.8M) for the loss and exposure of 46K customer records

Step 5: *"Govern Responsibly"*
Things you can do



5 Govern responsibly

4 Drive operational excellence

3 Have a plan

2 Understand where you are today

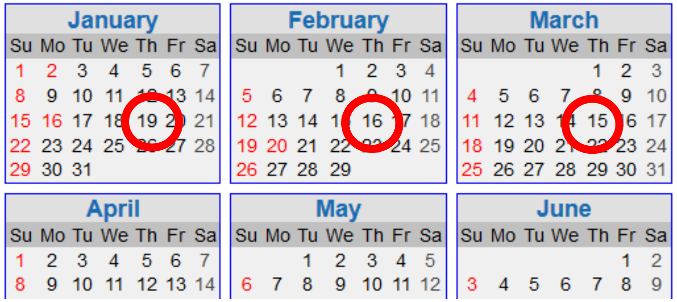
1 Know where you are going

Make application security part of your *sponsor's* day-to-day business

1. Make security one of your KPIs

3. Integrate into your overall security intelligence

2. Measure and report regularly



January						
Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

February						
Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29			

March						
Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

April						
Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14

May						
Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12

June						
Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9

Closing thoughts

- Better application security is necessary and achievable
- Vulnerable applications are a primary source of security breaches
- Security is no longer a technical problem, it is a board problem
- A successful application security program extends your current processes instead of creating new ones
- Demonstrate successes before expanding too broadly

ibm.com/security