Disclaimer

The information provided in this Presentation is owned by Reed Business Information Limited (“RBI”). The contents of this Presentation shall be treated as confidential and proprietary information and the Presentation should not be shown, read or used by any third party other than ‘You’ and your ‘employees’ on a need-to-know basis.

Ideas and concepts contained in this Presentation shall only be used with RBI’s written permission. All intellectual property rights in this Presentation remain vested in RBI and any references to third party trade names or trade marks in our Presentation, save where expressly provided, is neither an assertion of ownership or representation of an association with the owners of such trade names or trade marks.

The information contained in this Presentation may be obtained from public sources and information that our customers have provided to RBI. Any analysis, forecases, projections and opinions are based on such information and RBI have not verified the accuracy and completeness of the information. In no event shall RBI be liable for any indirect, consequential, special or incidental damages which may arise from the use of the information, even if advised of such possibility.

This Presentation is subject to contract and all warranties whether express or implied by statute, law or otherwise are hereby disclaimed and excluded to the extent permitted at law. In the event that the scope of the services change, this Presentation may require corresponding amendments. Any rights and obligations that may arise under this Presentation shall be governed by the laws of England and Wales and the Courts of England and Wales shall have non-exclusive jurisdiction to adjudicate any disputes arising here under.

5 June 2019

Security Best Practices

Edgardo Yap

Project Director, Professional Services, APAC, Accuity

Today's Discussion Topics

Risks & impacts of security vulnerabilities and threats to businesses

How is Accuity handling application security risks in its own business?

Do you know in which areas security threats reside in your business?

How security improvements are now embedded into the Accuity SDLC

Impacts of Accuity "zero-tolerance" on our product development

Engaging Accuity Professional Services to discuss your upgrade options

Question & Answer

Lets start with a little quiz…

What does C.I.A mean in the world of Information Security?

A Confidentiality, Integrity, Availability

B Complexity, Integrity, Authentication

C Confidentiality, Impact, Availability

D None of the above

What does C.I.A mean in the world of Information Security?

A Confidentiality, Integrity, Availability

B Complexity, Integrity, Authentication

C Confidentiality, Impact, Availability

D None of the above

What is NOT described as an ‘information asset’?

A Laptop

B Database Server

C Receptionist

D Microsoft Office

E All of the Above

F None of the above

What is NOT described as an ‘information asset’?

A Laptop

B Database Server

C Receptionist

D Microsoft Office

E All of the Above

F None of the above

Which of these characteristics create the best password policy?

A Passwords with 8 characters or more

B Passwords with Alpha-numeric characters

C Passwords with special characters

D All of the above

E None of the above

Which of these characteristics create the best password policy?

A Passwords with 8 characters or more

B Passwords with Alpha-numeric characters

C Passwords with special characters

D All of the above

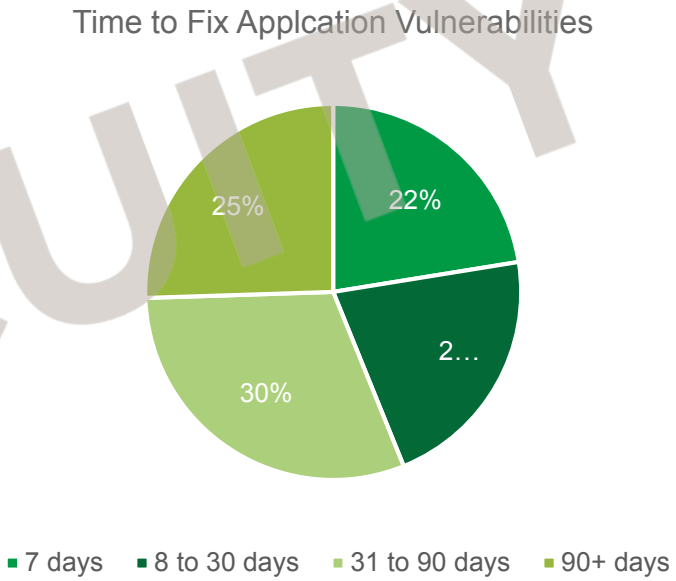
E None of the above

Risks & impacts of security vulnerabilities and threats to businesses

Some context…

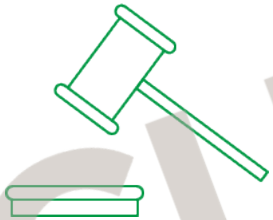
- 17,000+ new vulnerabilities in 2018
- Approximately 47 new vulnerabilities per day
- 2018 saw a 23% increase compared to 2017
- 20% of Application Vulnerabilities are High or Critical risk
- Average of 67 days to close a vulnerability

Sources: edgescan Vulnerability statistics report
www.imperva.com – State of Web Application Vulnerabilities



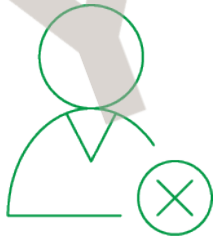
Risks & impacts of security vulnerabilities and threats to businesses

Serious commercial impact in the event of a security breach to both us as an organisation but equally to our customers.



Legal and Compliance breaches can end up in lawsuits and fines.

Under the GDPR laws,
The CNIL's restricted committee imposed a financial penalty of 50 Million euros against GOOGLE LLC.



Damage to reputation can be terminal that could take many years to recover from and in some cases never.

Typically, 60% of Small Businesses will fold within 6 months of a Cyber Attack.

Risks & impacts of security vulnerabilities and threats to businesses

Top 10 Breaches in 2018

#	Breaches	People Affected	Disclosed
1	Aadhaar	1,000,000,000	January 2018
2	Starwood-Marriot	500,000,000	September 2018
3	Exactis	340,000,000	June 2018
4	Under Armour - MyFitnessPal	150,000,000	Febuary 2018
5	Quora	100,000,000	December 2018
6	MyHeritage	92,000,000	June 2018
7	Facebook	87,000,000	September 2018
8	Elasticsearch	82,000,000	November 2018
9	Newegg	50,000,000	September 2018
10	Panera	37,000,000	April 2018

Sources: https://blog.avast.com/biggest-data-breaches

Some of the recent data breaches from 2018 and 2019

BRITISH AIRWAYS

Stolen data included personal and financial details of over 380k British Airways customers.

AADHAAR

A breach where personal info (photographs, national ID numbers, phone numbers, addresses, postal codes, and email addresses) of 1.5 billion Indian citizens were exposed.

540 million Facebook users exposed in breach announced in 2019 where user records were publicly exposed in two app datasets that were digitally stored in two Amazon Simple Storage Service (S3) storage buckets.

DOW JONES

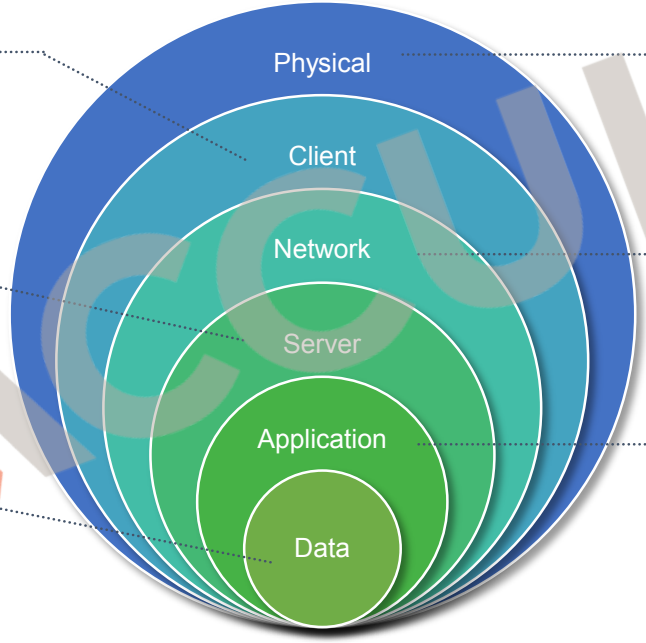
An independent researcher, discovered that an AWS hosted Elasticsearch database exposed the records including Dow Jones' Watchlist database, which companies use as part of their risk and compliance efforts.

Do you know in which areas security threats reside in your business?

- No system locks
- No anti-virus
- External storage devices

- Missing Patches
- No Firewall
- Local privilege

- Default credentials
- No redundancy
- Missing Patches



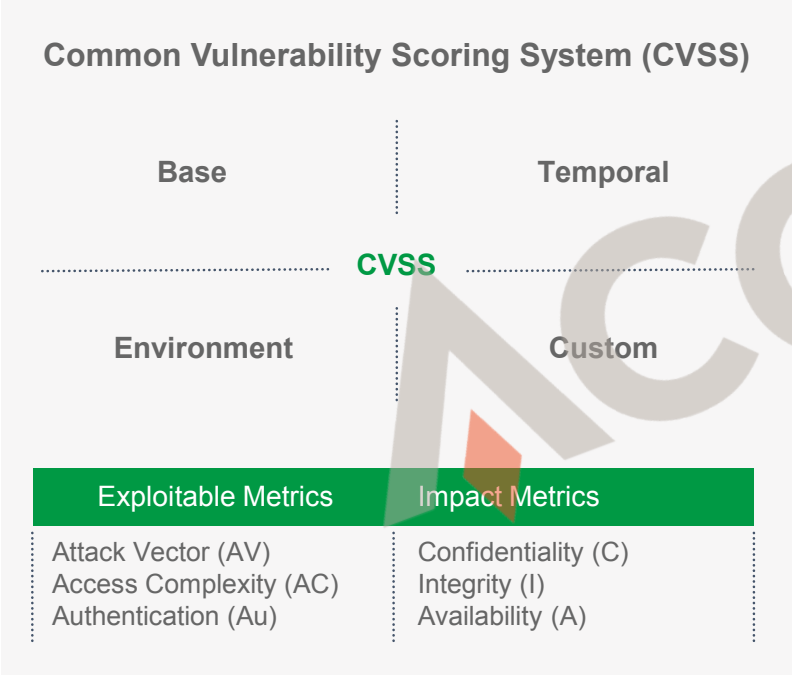
- Written passwords
- Social engineering
- Access to server rooms

- Exposed remote terminal services
- FTP exposure
- Telnet protocol

- Cross-Site Scripting
- HTML injection
- Session management

How you can help improve security in your business systems

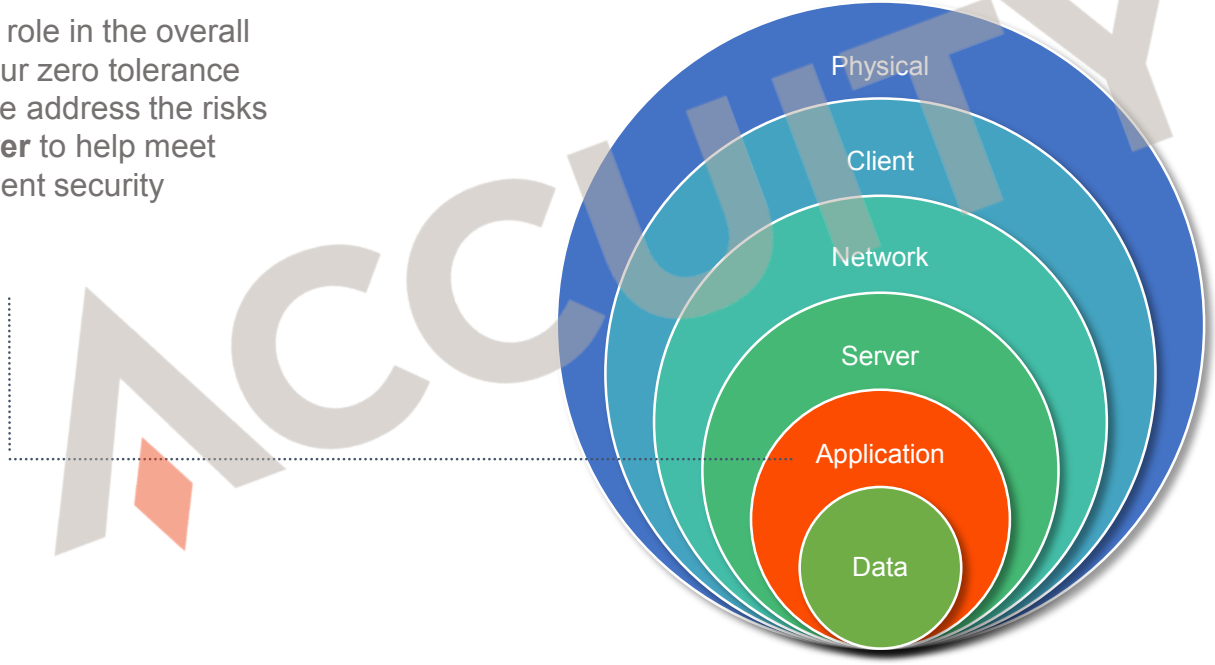
…using risk based approach to prioritize vulnerability resolution.



Vulnerabilities	Score	Cost to resolve
Missing Patches	9.6	30,000.00
No redundancy	9	300,000.00
No Firewall	8.5	150,000.00
Default credentials	8	50,000.00
No anti-virus	7.8	275,000.00
Exposed remote terminal services	7.4	80,000.00
Access to server rooms	6.2	425,000.00
External storage devices	5	120,000.00
No system locks	4.8	-
Local priviliege escalation	4	5,000.00

How you can help improve security in your business systems

Accuity plays a critical role in the overall security framework- our zero tolerance initiative means that we address the risks in the **Application layer** to help meet your institution's stringent security framework objectives



How is Accuity handling application security risks in its own business?

Our Focus

1. We aggressively address vulnerabilities across our portfolio of products utilising industry recognised processes and tools to minimise security and privacy risks for our customers.

2. We continue to significantly invest in our security programme, looking at areas for enhancement in technology, process and skills.

3. We are actively developing and enhancing our scanning process using static code analysis, web application testing, penetration testing and open source scanning.

4. We actively review and implement tailor made security curriculums for all our staff to further enhance our capabilities to deal with security related issues.

How is Accuity handling application security risks?

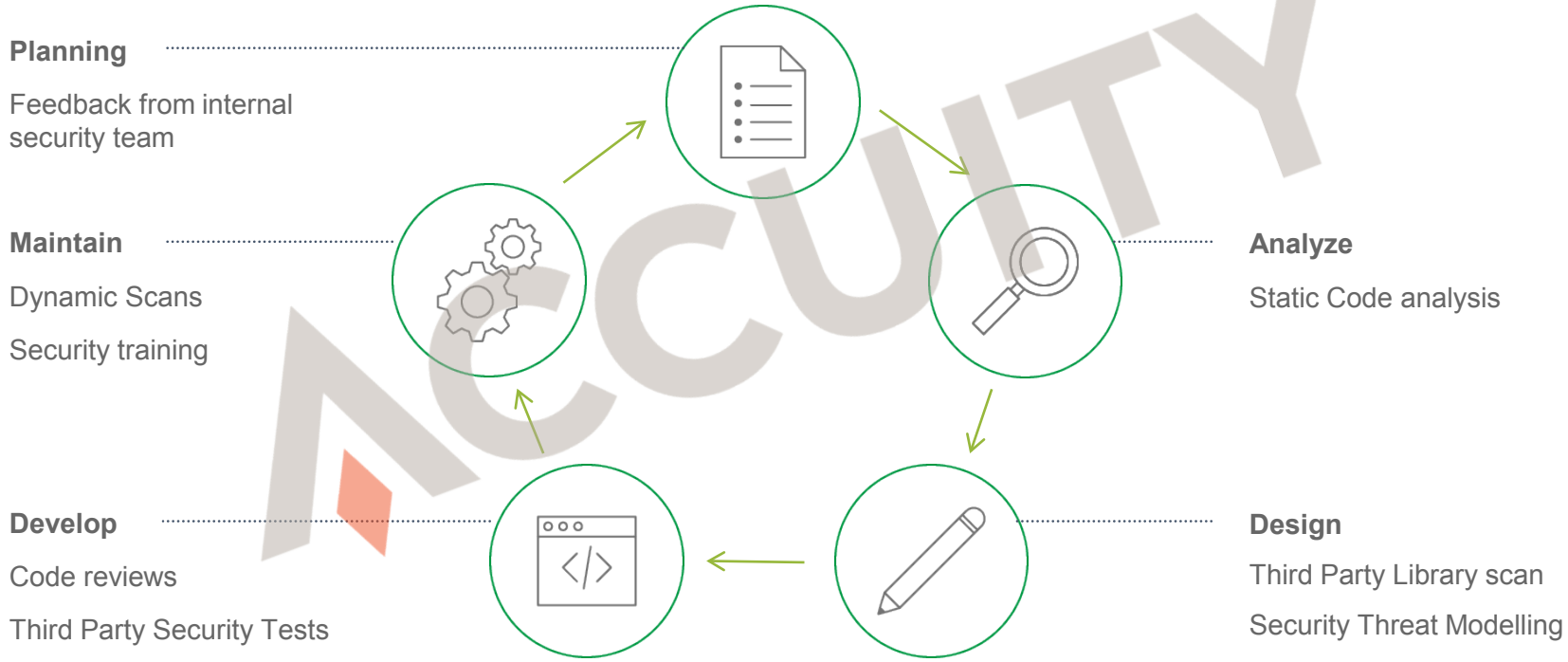
Our Approach

We have taken a two staged proactive approach to remediate security vulnerabilities in all of our products including expanding our finding capabilities and plans to progress fixes.

We actively track vulnerabilities within our products and take a risk based approach to progressing the remediation work.

We have a cadence of more frequent security updates and releases with emphasis for our customers to upgrade on a more frequent basis

Security improvements are now embedded into the Accuity SDLC



Impacts of Accuity ‘zero-tolerance’ on our product development

More Secure

More application vulnerabilities will be resolved for the benefit of our customers

Better Releases

Products with stronger security enhancements lead to best value for clients on each release

Enhancements

With vulnerabilities being resolved, there will be opportunity to consider more value add enhancements

Confidence

Products seen to add great value and security inspire even greater confidence with our clients

The Accuity commitment to our clients

1

We are committed to ensuring that your information is secure and protected. We use a variety of administrative, physical and technical security measures intended to safeguard your personal information.

2

We are committed to work with our customers in order to assess and progress any security related issues or otherwise aligned with our InfoSec policies and product roadmap deliveries.

3

We have a strong software development lifecycle process however we are committed to review the process on an ongoing basis in order to continuously improve our abilities to deliver secure products to our customers.

Engaging Accuity Professional Services to discuss your upgrade options

3 options to reach out to Professional Services Group to scope out your upgrade initiatives:

1. Contact your Account Manager
2. Contact your Professional Services Consultant
3. Contact Support:

   support@accuity.com – For **Firco Compliance Link** products

   support@fircosoft.com – For **Firco Enterprise** products

Things to prepare prior to your discussion with Professional Services Group:

1. Existing Firco solution/modules and versions currently utilised
2. Volumes of business under discussion - such as no. of accounts/transactions
3. Existing services setup/configuration
4. Existing architecture/technology stack set up (versions etc.)

Thank you for your attention

Take a break

The Summit will resume in 30min.