MELBOURNE IT

/ PRESENTATION /

ARE YOU AT **RISK?**

Everything you need to know to secure your web presence.

THE CURRENT **THREAT LANDSCAPE**

Mega attack

- A DDoS attack which is greater than 100Gbps.
- This is extremely large and we (Akamai) hardly ever saw them a couple of years ago. In Q3 2014 we saw 17 on one single customer.
- This is fairly new in terms of volume.

SQLI and XXS tools

- These days it is much easier to launch attacks – no technical knowledge is needed, and online tools can be used, which are inexpensive.

Multi Vector

- The hacker is using more than one attack vector to bring down the victim – e.g. a combination of volumetric DDoS and SQL injection.
- The DDoS attack would occupy the security team, so it may not notice the SQL injection.

Criminal Actors

- Credit card credential theft is on the rise but we are also seeing a lot of corporate espionage – potentially launched by state sponsored organisations.

Case Study – Shellshock 2014

- Akamai found out about Shellshock and had all vulnerabilities patched before the vulnerability even became public. Akamai's Web Application Firewall (WAF) was updated to deliver a virtual patch to customers within hours after the public announcement.

IMPACT OF AN **ATTACK**

- It’s not easy to classify hackers or the methods that they are going to use.
- Distribute.IT example
  - An Australian trading platform was founded in 2002 by the Woerndle brothers
  - By 2011 Distribute.IT had secured a 10% market share and more than 200,000 clients on its books

A hacker got access to master user privileges which = access to everything!

The website spent over 6 days offline to fix

First day after being back online, the main servers were intermittently offline.

The hacker had regained master user privileges and defaced site via VoIP and PHP vulnerabilities.

The company was nearly bankrupt

Both Woerndle brothers lost their homes

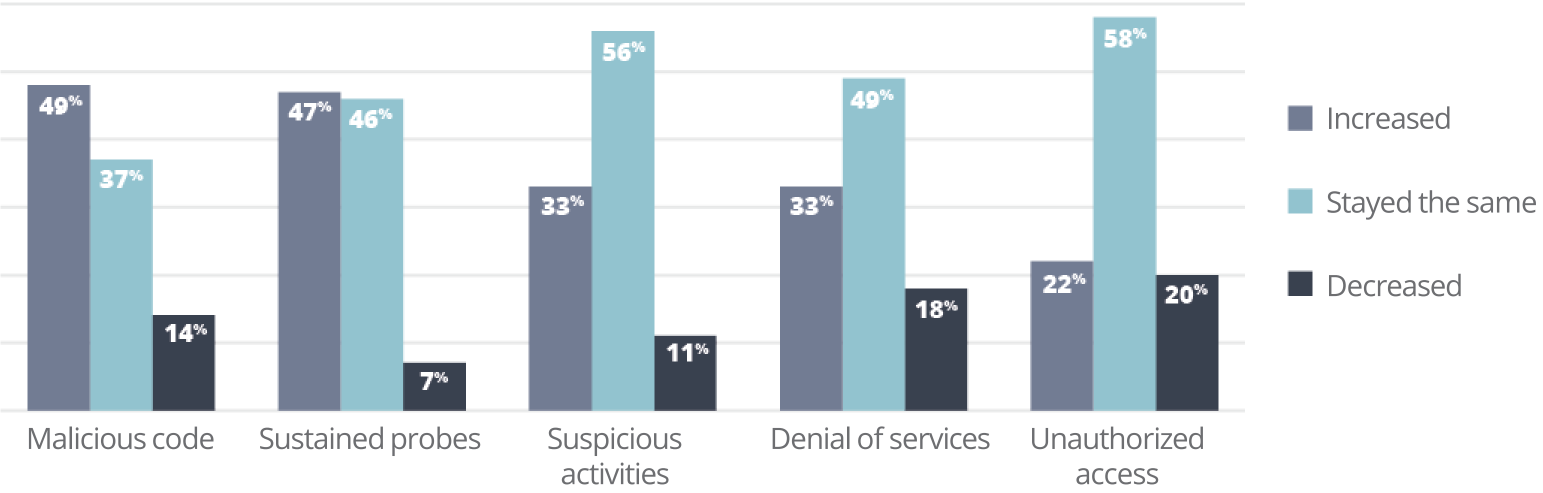
- Hacker = an unemployed truck driver who learned from YouTube and chatrooms

IMPACT OF AN **ATTACK**

Results from Ponemon 2014 Study

- Results from Ponemon 2014 Study
- 2014 Results: 314 companies interviewed, results do not disclose any company names

Changes in security threats over the forthcoming year



- Results are for companies in 10 countries in North America, Europe, Asia and Australia, across 16 industries

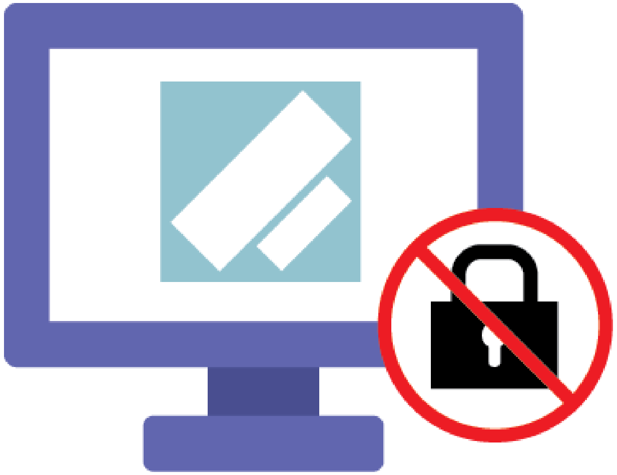
Australian Specifics

- 22 Case Studies analysed
- $3M AUD average breach cost

DON'T **BE THAT GUY**

What not to do

- A lot of businesses think that they have nothing of value.
- So why do companies still have server rooms locked?
- Why set passwords on servers and end user terminals?



Case Study – Home Depot

- Home Depot forgot that their point of sale (POS) network was IP enabled. Now they're facing multimillions of dollars in losses. You might not have a POS system in your network, but a full profile with a person's name, address, phone number and date of birth alone, is worth around $3.
- If you have 1000 employees, that's an easy $3k for a hacker if they can get it. Add in a bank account number or a credit card, and you can be looking at up to $150 per record.

UNDERSTANDING **THE ATTACKERS**

- Different groups have different motivations.
  - Three examples:

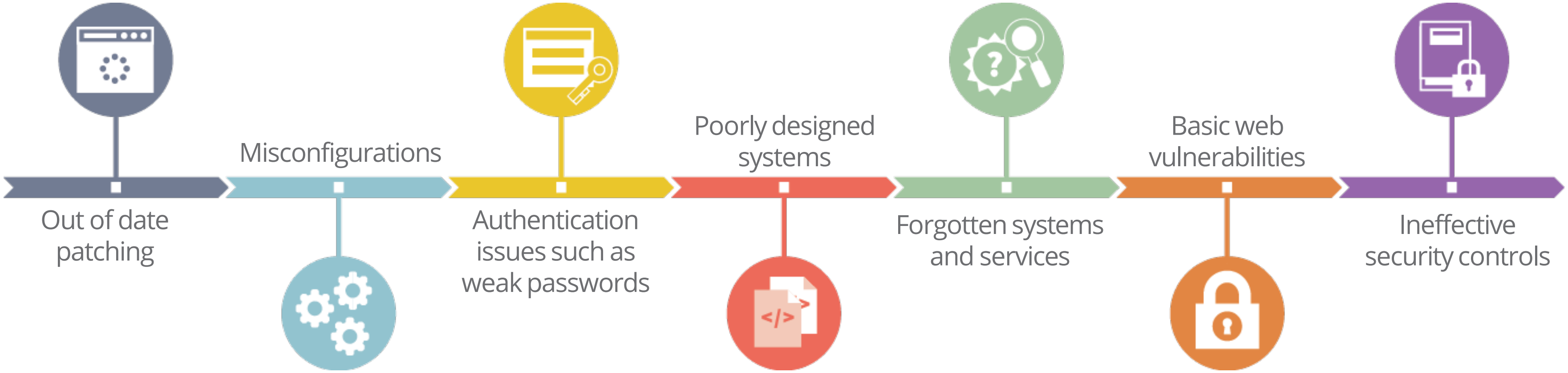
	Cyber Crime	Hacktivists	Advanced Persistent Threat (APT) style
GOAL	Make money	Spread a message. Cause embarrassment and brand damage	Steal intellectual property from government and corporates
HOW	DDoS extortion, financial theft (credit cards), personal data sale	Deface websites. Dump company specific internal information	Advanced, well planned, long term attacks
	• Understands certain hacking methodology or vulnerability • Willing to move to another target if protection level high	• High level of attention / press is key • Willing to move to another target if protection level high	• Nearly impossible to thwart • Well thought out Incident Response Plan key is required for this type of attack

- Ultimately it's a risk reward industry. Any attacker wants a good ROI.

- What attackers do we see the most often?
  - Remote scanners looking for vulnerabilities.

THE **VULNERABILITIES**

- The attackers are often exploiting the following:


Out of date patching
Misconfigurations
Authentication issues such as weak passwords
Poorly designed systems
Forgotten systems and services
Basic web vulnerabilities
Ineffective security controls

WHO'S GOING
TO THREATEN ME AND MY COMPANY?

- Threats come from many different sources, and can be broadly grouped into three classes.
  - Random
    - This is where the attacker doesn't know who they're attacking, and in some ways, they don't care. It's all about spray and pray, because the effort is so low, and so cheap, they can afford to send out 10,000 emails, to get one victim. Random attacks include things like Cryptolocker and Script Kiddies (people who don't have any technical knowledge, using easy-to-use tools).
  - Opportunistic
    - Attackers are slightly more selective. They have better skills, or a position of trust, and they've gotten access to a machine or group of machines. This can include when someone has found a vulnerability through scanning, and have put it up for sale.
    - For example, if there's an SQL injection that will dump the contents of a customer database or an employee database, that can be sold for big money. Likewise, if someone has phished or brute forced some working credentials to get into a system through a remote login, they can sell this.
    - This kind of access can either be for the direct theft of data, or for extortion.
  - Targeted
    - It's very difficult to avoid being the victim of a targeted attack. 'Anonymous' hacking group is an example of this – with many examples in the press. Anonymous is doing it in their own time for a political reason. Imagine if the attacker was state sponsored, it was a paid full time job, with good access to tools and training.

CURRENT HIGH RISK **TYPES OF ATTACK**

- High risk - depends on your company and the organisation you're working for

Where is the content?	What would pose the greatest financial impact if it were to be breached or go offline?
Which systems, which data?	Question of data becoming unavailable or question of data being leaked?
Technology Q's to consider	Do you have issues around infrastructure being able to handle a large amount of traffic? Do you have some security in place but not capable of handling a slow get, or slow post attack?
Operational DB	Do you have a DB which is a critical piece of your daily operations?
Once identified systems	What do I need to do to protect those and how much is going to cost me? Is it possible to infiltrate critical systems via non-critical unprotected path?

- Top tips

- **CREATE A RISK PLAN**
  - Where are the vulnerabilities?
  - How much is it going to cost me?
  - What's the risk of an attack?

- **CREATE AN INCIDENT RESPONSE PLAN**

KEY CONSIDERATIONS FOR
A RESILIENT WEB SECURITY STRATEGY

- How do I respond?
  - There are different strategies for different risk profiles:

Everyone has to protect against random attacks. No exceptions.

If you have an internet presence, you need to consider where the opportunities are to attack and mitigate, reduce or accept the risk.

If you have something worth stealing by determined cybercriminals or foreign entities, you need to consider how to defend against that.

STRATEGIES FOR **DIFFERENT RISK PROFILES**

Random Attacks	Opportunistic Attacks	Targeted Attacks
• Establish a solid basic security antivirus/firewalls/ web filtering • Emphasise safe online behaviours through training	• Understand and reduce your “attack surface” • Perform Penetration Tests	• Ask yourself - Does this information need to be on the Internet? • Use global threat intelligence • Use APT\exfiltration detection tools
Gotchas		
• BYOD and rogue devices can be a weak point • Excessive permissions exacerbates problems	• Admin interfaces on CMSes being made public • Remote access using only username/password	• Everything …!

KEY **DEFENSE STRATEGIES**

- There is no magic security silver bullet.
  - There are however multiple effective, and cost appropriate layers in the solution.
- Get the basics right.
  - Handle data appropriately. Patch your systems. Enforce complex passwords.
- Design systems assuming it will be compromised.
  - This may sound bad, but it makes for better designs.
- Ask questions of your service providers.
  - Understand who is responsible for what.
- Report security incidents to relevant authorities.
- The biggest mistake organisations make is assuming it won't happen to them.

KEY **CONSIDERATIONS**

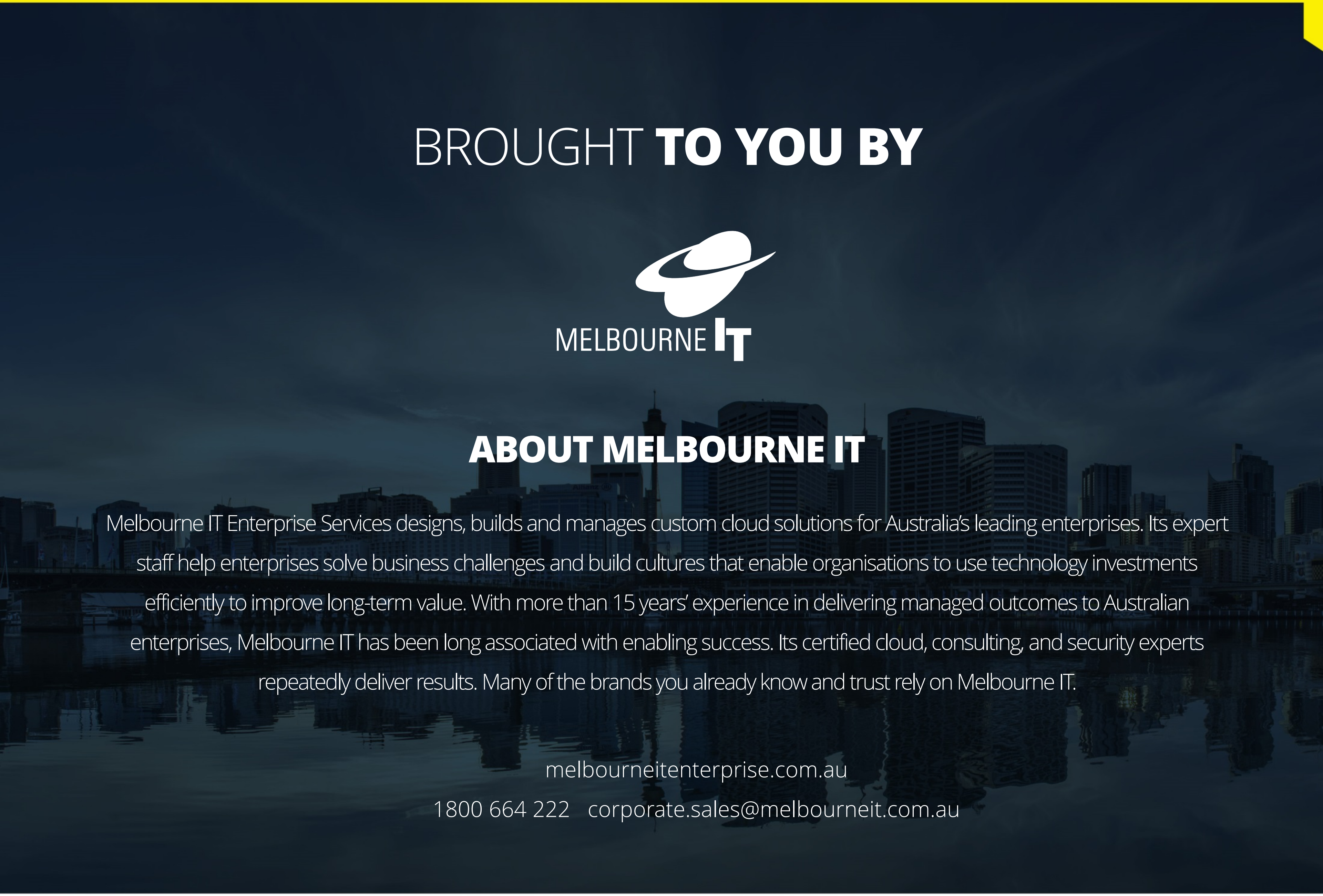
- What are the key components of a resilient security posture?

- Have someone on the board who represents the topic of security
  - someone who has security as their main concern.
- Look at your organisation
  - where your risks are, take a serious methodology of risk and probability of being attacked and develop a business plan that is relevant to your organisation.
- DDoS, Application Layer protection
  - Consider both company Datacentre as well as cloud based applications.

- How can I build security into my development process?
  - You may have development in-house, may outsource it - this can be something that doesn't cost a lot of money but brings a lot of advantages
- Be ready for an attack
  - protect and mitigate as much as possible but have something in place to react accordingly. Who do I need to tell about the breach and who is responsible for that?
- Continual Improvement

RESOURCES

- Australian Signals Directorate (ASD) TOP 4
  - asd.gov.au/infosec/mitigationstrategies.htm
- SANS Critical Security Controls
  - sans.org/critical-security-controls/
- Cloud Security Alliance
  - cloudsecurityalliance.org



BROUGHT **TO YOU BY**

MELBOURNE IT

ABOUT MELBOURNE IT

Melbourne IT Enterprise Services designs, builds and manages custom cloud solutions for Australia's leading enterprises. Its expert staff help enterprises solve business challenges and build cultures that enable organisations to use technology investments efficiently to improve long-term value. With more than 15 years' experience in delivering managed outcomes to Australian enterprises, Melbourne IT has been long associated with enabling success. Its certified cloud, consulting, and security experts repeatedly deliver results. Many of the brands you already know and trust rely on Melbourne IT.

melbourneitenterprise.com.au

1800 664 222 corporate.sales@melbourneit.com.au