Simplifying Security:

Protecting your Clients and your Company

Who Dat?

Drew Gorton

@dgorton

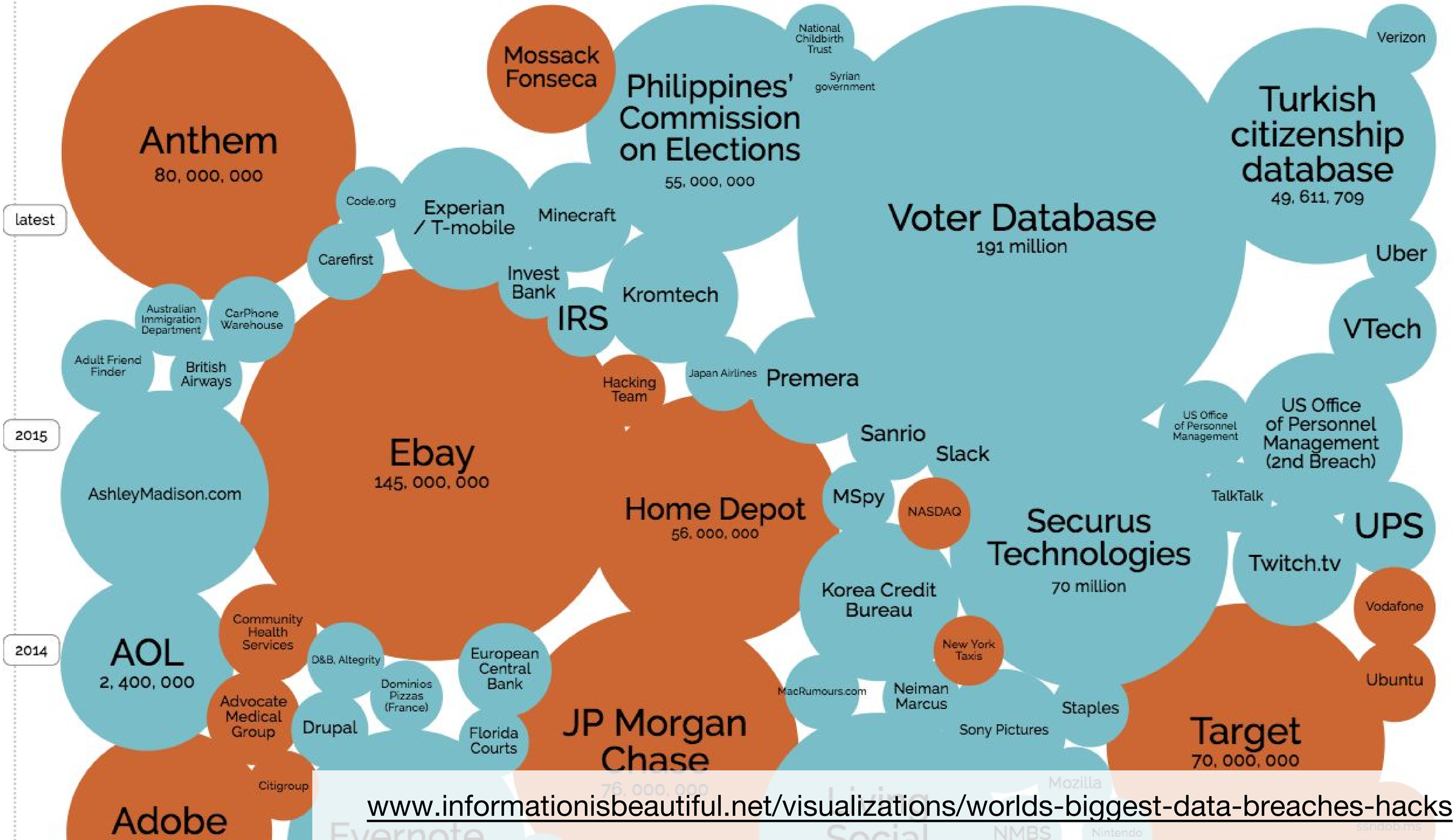
Luke Probasco

@geetarluke

Chris Teitzel

@technerdteitzel

Time For a Quick Game



www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

Home | Notify me | Domain search | Pwned sites | Pastes | API | About | Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username

pwned?

103	345,003,107	36,213	26,567,837
pwned websites	pwned accounts	pastes	paste accounts

www.haveibeenpwned.com

Because that is where the money is.

- Willie Sutton

Take Aways

- Breaches aren’t a matter of “if”, but “when”
- Protect more than credit cards - that’s not what hackers really want anyway

Five Common Security Myths

I’m too small to be a target.

Private businesses
are not regulated.

Encryption is complicated.

Security kills performance.

My clients aren’t
paying me for security.

Take Aways

- Hackers are targeting small and mid-sized organizations
- Compliance covers all industries
- You need to build security into sites, client’s shouldn’t have to ask for it
- It’s not that hard

Security Fundamentals

What is Security?

PANTHEON®

CIA Triad

- Confidentiality
- Integrity
- Availability

Security is a Continuum

- More vs. Less
- Not On vs. Off

Personally Identifiable Information (PII)

Information that can be combined with something else to determine a specific person:

- **Name, address, email, date of birth, telephone number, company, title ...**

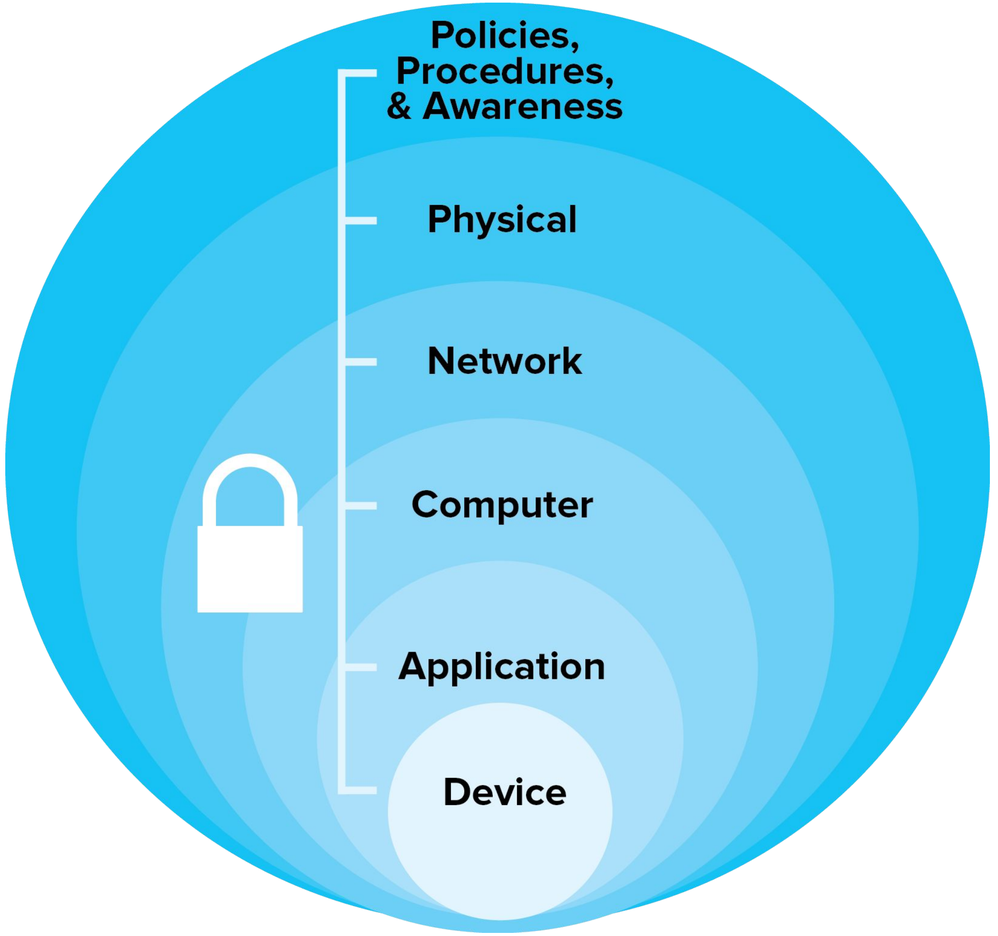
Some compliance regulations specify what data

Don’t build Death Star security.

- David Strauss

Defense in Depth

- Each layer takes time, which is the enemy of hackers
- Involves every portion of the company



http://www.slideshare.net/warpforge/dont-build-death-star-security-oreilly-software-architecture-conference-2016-nyc

Take Aways

- There is no security “magic bullet”
- Have a “defense in depth” approach
- If you don’t have to collect or store it, don’t

Security is Good for Business

Business Wins

- Stand out in your proposals
- Win more RFP’s
  - Larger RFP’s usually require attention to security
  - Add into proposals even when not asked for it

Business Wins

- You can be liable for a breach
- Reduce your risk by implementing proper security
  - Even if the client doesn’t ask for it
  - Even if you have to eat the cost

Business Wins

- Minimize exposure to sensitive client data
  - Don’t store passwords
  - Don’t hold onto credentials
- May mean telling a client no or that you cannot do what is asked

Business Wins

- Build a name for yourself
- Security is a growing niche
- Security builds trust and clients who trust you are clients who refer you

Business Fails

California Data Breach Report, 2012 - 2015

Recommendation 1: The 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.

Everyone has the right to the protection of personal data.

General Data Protection Regulation (GDPR) - EU

Take Aways

- Win more and larger projects
- Security can be one more tool in tool belt
- Protect your business by protecting your clients
- Growing niche

Questions to Ask Your Clients

Questions to ask your clients

What information is collected?

Who will have logins?

Anything being sold? Any donations?

Trigger Words

- Ecommerce
- Donations
- Integration
- API
- Registered Users
- Paywall
- Forms in general

Take Aways

- PII is more than Credit Cards
- Use Discovery to uncover security concerns
- Dig in deeper on trigger words

Creating a Culture of Security

Creating a culture of Security

Every person on the team is responsible for their part to be secure

Creating a Culture of Security

- Sales/Marketing
  - Use services and vendors that have been vetted for security (payment gateways, cloud storage etc.)
  - Website responsibility is usually under Marketing
  - When in doubt, don’t post it
  - Get away from FUD, instead use security to empower

Creating a Culture of Security

- Development Team
  - Allow for time spent researching/learning
  - Regular code audits
  - Award and recognize failures caught by the team
  - Involve the development team in every proposal to ensure the right questions are asked

Creating a Culture of Security

- Practical Tips
  - Use password managment tools
  - Use single sign-on / 2FA for all business critical items
  - Keep internal and guest wifi separate (don’t give out wifi to everyone who walks in the door)
  - Regular security audits, discussions, memos etc.

Take Aways

- Everyone is responsible for security, not just developers
- Communication is key, encourage it!
- Learn from failures!
- “Your focus on security keeps us all secure”

Security Profiles & Case Studies

PANTHEON®

Profile:

Small Business

Site: Brochureware, MailChimp, PayPal, no users

Focus on: Hosting platform, Drupal, API Keys

PANTHEON®

Profile:

Higher Education

Site: Admissions, student records, donations

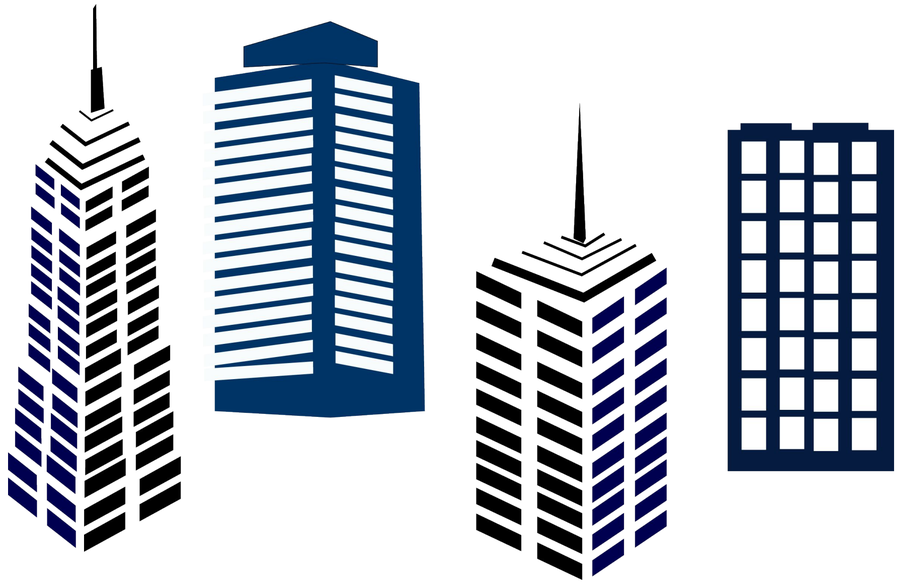
Focus on: Encryption, key management, compliance

Security Profiles & Case Studies

PANTHEON®

Profile:

Enterprise



Site: Corporate site, intranet, sub-sites

Focus on: Hosting, 2FA, encryption, key management, compliance

Take Aways

- Sites large and small have similar security concerns
- Modules and services can help
- Security is a good business investment

Evaluating Hosting Platforms

Drupal™

Search …

Log in / Register

Marketplace

Services | Hosting | Training | Books | Supporters

Drupal Shared Hosting

bluehost 1-CLICK Drupal ONLY $2.95

Bluehost: Exclusive for Drupal users only $2.95/month! 50% OFF!

As the leader in open source hosting technology, Bluehost is the best shared hosting provider available. Use the MOJO 1-click installer to start using Drupal and keep things up to date. And, when you sign up for a hosting account through this page, Bluehost will donate your hosting fee back to **Drupal.org!**

Premium Supporter

SiteGround DRUPAL HOSTING

Drupal Hosting Crafted With Care

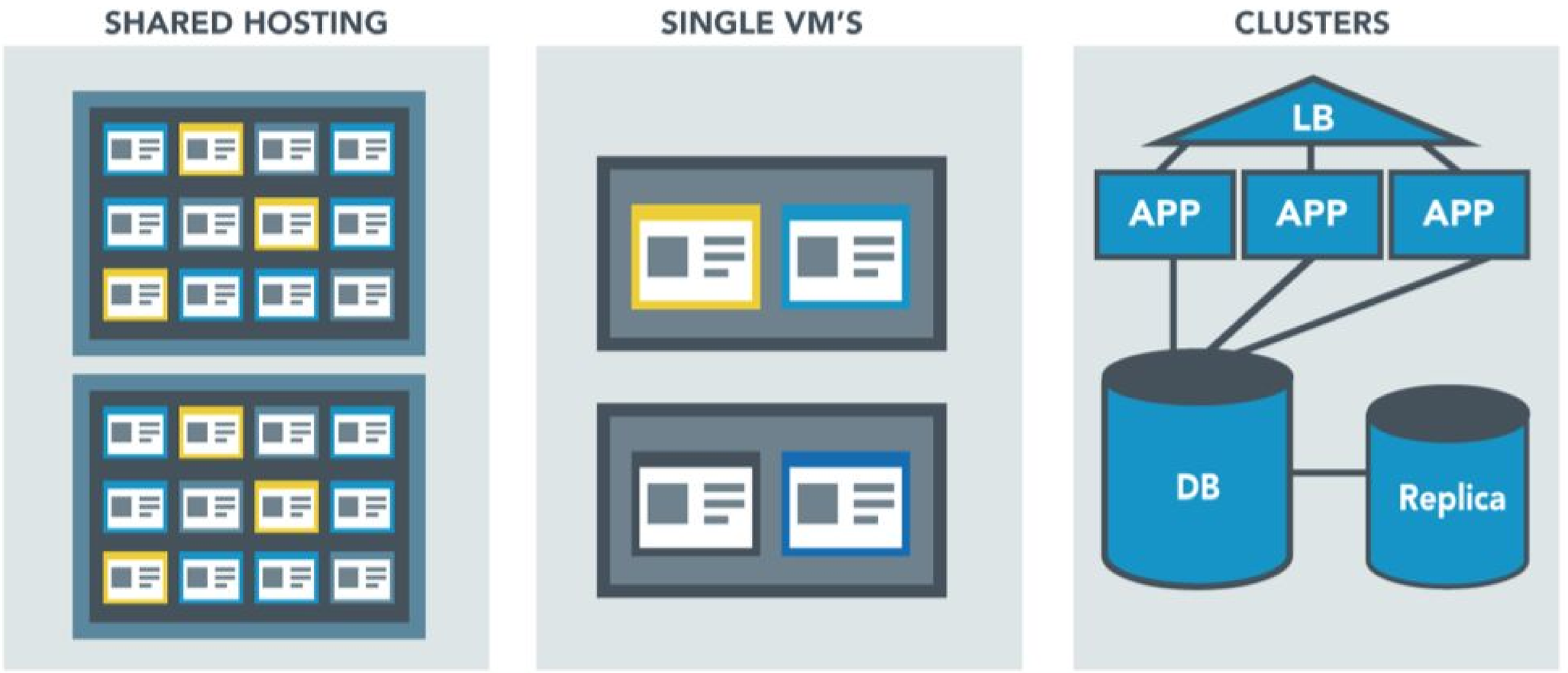
SiteGround web hosting company is known for the expert and fast support it provides 24/7. We offer free Drupal migration or installation, and resolve issues with your

Premium Supporter

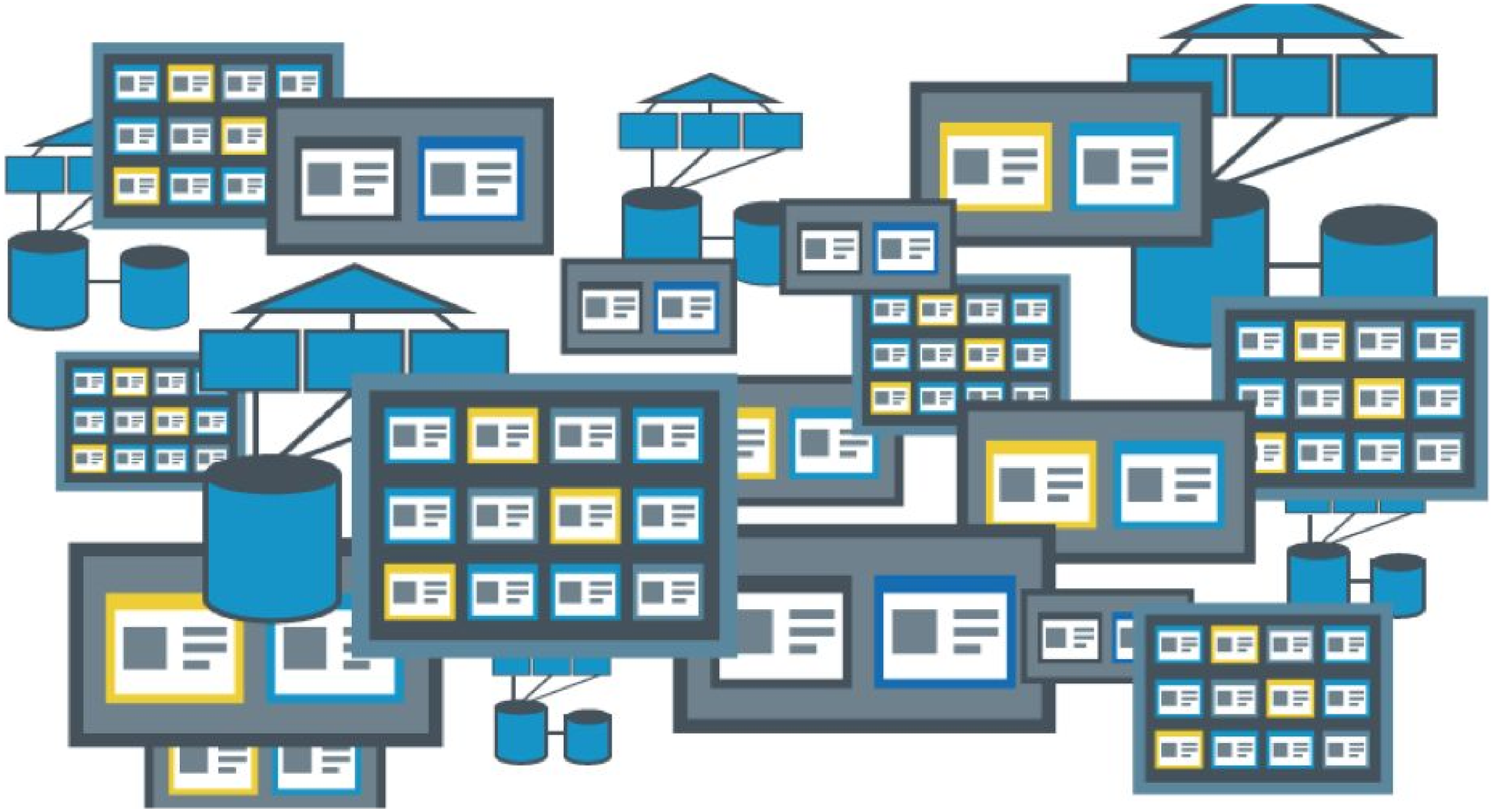
- Shared Hosting
- Managed/Enterprise Hosting
- Cloud Hosting
- VPS Hosting
- Dedicated Hosting

https://www.drupal.org/hosting

Traditional Options



Real World Mess



Better Way: Cloud. Consistent, Scalable

Take Aways

- Start with Drupal.org
- No Shared Hosting!
- Ask about Drupalgeddon process, timeframe, results
- Ask about Heartbleed process, timeframe, results

Securing Drupal

Secure Configuration

- **Secure User 1**
  - No simple passwords
  - Don’t share passwords across sites
  - Doesn’t have to be ‘admin’
- **Permissions & Roles**
  - Administer * is powerful
  - Administer filters can pwn site
- **No PHP (!!!)**
- **Update module**
  - Wednesdays are security releases
  - Turn it on. Get the notifications. Do them

Drupal Modules (1 of 2)

- **Password Policy** + **Password Strength:** enforce strong passwords
- **Security Review:** tests for easy-to-make configuration mistakes
- **Security Kit:** security-hardening options
- **Hacked!:** check for altered code
- **Paranoia:** identify and block PHP evals
- **Permissions Lock:** more granular control over 'Administer Permissions'

Drupal Modules (2 of 2)

- **Login Security:** limit login attempts
- **Automated Logout:** force logout after a specified time of inactivity
- **Two Factor Authentication:** base module for two-factor authentication
- **Encrypt:** provides an API for performing two-way data encryption
- **Key:** gives site administrators the ability to define how and where keys are stored

Migrate to Drupal 8!

Drupal 8 FTW

- Drupal 6 is EOL
  - Great update opportunity
  - Migration is focused first on 6 -> 8 compatibility
  - Fix mistakes in the upgrade - don’t just keep bad practices in place

Drupal 8 FTW

- Drupal 8 is the most secure Drupal
  - Core isn’t an island anymore
  - String sanitization
  - NO PHP IN CORE!
  - Twig - No more bad practices!

90% of site-specific vulnerabilities are in the custom theme

- Peter Wolanin

https://dev.acquia.com/blog/drupal-8/10-ways-drupal-8-will-be-more-secure/2015/08/27/6621

Drupal 8 FTW

- Upgrade Cycle is a great opportunity for businesses to sell
- Built in REST API
  - Secure access to data
  - Opportunity for expanded projects

Take Aways

- Drupal 8 is newer, faster, and more secure!
- Upgrade opportunity from Drupal 6 -> 8 to fix issues and add new business
- Expand projects with API support (be careful what you expose)

Bringing It Full Circle

In Conclusion

- ✓ You and your clients are targets
- ✓ Business value of security
- ✓ Build security into your processes, culture, proposals and billing
- ✓ Use a secure hosting provider
- ✓ Improve Drupal’s security with Configuration + Modules

Rate this Session and Get the Slides

https://events.drupal.org/neworleans2016/sessions/simplifying-security-protecting-your-clients-and-your-company

Questions?

PANTHEON®

Drew Gorton
@dgorton

Luke Probasco
@geetarluke

Chris Teitzel
@technerdteitzel