Software Applications for Business are not the same as social media apps - Security must be Built-in, not Added-on

Developing new applications to sharpen your edge has never been easier; software developers are almost under every rock. That's why software development is a more treacherous minefield than ever.

'One of the big problems in IT right now is that security and compliance are generally handled at runtime and are not part of the entire software development workflow. Security and compliance are an afterthought rather than an active part of the development lifecycle.' Tony Bradley, Editor-in-Chief, TechSpective.net

Facebook, Mariott Hotels, MyHeritage, British Airways and MyFitnessPal are just five of a spate of recent high-profile data breaches overseas. Down Under, we've scored a few too, such as the South Australia Blood Bank and Victoria's Emergency Services. The MyHealth Network was uniquely spectacular: some 40 data breaches in 2018 alone. Even the Christchurch disaster victims had their privacy compromised.

What I want to focus on here is that most of these breaches were entirely preventable, and not the work of genius level hackers. More importantly, we touch on how the requirements for custom software for business, government agencies and universities are substantially more onerous than what might apply for a free car parking app.

Convenience has a Price

The fact that Facebook has bounced back from a disastrous 2018 shows that consumers have resigned themselves to the new reality; online privacy is a myth. Clearly, consumers think the convenience of internet and social media is worth the sacrifice.

If you run a business or a university or government agency, you can't take that attitude; a single data breach will cause serious damage to your reputation, revenues and share price. And the Australian Government's Notifiable Data Breach scheme has upped the ante, by applying hefty fines.

Social media is one vulnerability, but far more sophisticated threats are looming with the Internet of Things (IoT), Artificial Intelligence (AI), and mobile malware, however from what we've observed, most businesses lack the resources to deal with the current threats let alone future ones.

‘Computer security is broken from top to bottom’

That’s the heading of this article in The Economist. One statement rang a bell with me since it’s often an issue in organisations that approach us for help: ‘The innocent foundations of many computer systems remain a source for concern.’

Sensational headlines aside, even ageing legacy systems aren’t necessarily basket cases. Sure, if left untouched they will be – and leave gaping security holes. Yet, they can be made secure or replaced with systems that are secure by design. You just have to know what you’re doing.

If inexpert developers are under every rock, it’s no surprise that so many security systems are broken. Yet, it’s not true to claim that computer security is broken per se. The real issue is that it takes skill to write code that is secure from hackers.

Fundamental issues that leave obvious security gaps include new systems that were written without securing the code against exploits, or that have never been penetration or compliance tested, or even more common is systems on cloud platforms that can’t guarantee secure hosting within known jurisdictions.

Application Security Must Be Built-In

As we saw at the start, developers often treat security as an afterthought; they’re focused entirely on delivering new applications on time. That’s a serious mistake: if security and compliance are not part of the software development life cycle from the start, they won’t be up to scratch. In addition, it’s much more expensive to add security later, if it’s not nailed down in the original design and development.

‘The attackers only have to find one weakness,’ Kathleen Fisher at Tufts University told The Economist.’ The defenders have to plug every single hole, including ones they don’t know about.’ That’s so true.

Plugging the holes you don’t know about is tough, but that job is made possible by using methodologies like DevOps.

In simple terms, DevOps involves the building, testing, and deployment of applications along the lines of a production line. Using DevOps, security and testing can be automated via checkpoints along the production line allowing developers to routinely produce code that is secure and free of most bugs. It’s not hard when done this way.

Grab it and Run or Cheap Imitations

These days, we often deal with young folks who’re used to downloading whatever they need from the internet. The other common practice is having apps developed overseas; the price is alluring – especially if you think you’re getting the same result for a lot less. Usually you’re not. That’s a lesson quite a few of companies learn the hard way.

The sting is often in the tail of the project: support difficulties, documentation that lacks clarity due to developers' limited English, and cultural differences that mean that certain things that we take 'as read' Down Under, are not taken care of or even considered.

That said, keeping the project in Australia doesn't guarantee a perfect outcome either.

As we discussed in the last section, building quality business applications depends on trained engineers using rigorous processes. Experience plays an essential part too, as does a good command of English (for documentation), and knowledge of our laws regarding Governance, Risk & Compliance and Notifiable Data Breaches.

We also see businesses that have used sole contractors to write software, which

- Has proved difficult to integrate with existing systems
- Has seen only superficial acceptance testing, and no penetration or load testing
- Is difficult to maintain since the contractor took a full-time job in another city.

Inexperienced, low cost developers are everywhere. They don't fully understand the problem domain, or aren't trained in the latest development techniques, or they cut corners to meet budget, so things like non-functional requirements, scalability, version support, usability, performance and storing sensitive data are not their primary concern.

In software development if the price seems too cheap, there is likely good reason.

Enterprising Mobile Apps

The story gets more complicated with mobile apps, which are offered by organisations ranging from banks and betting shops to your local council and coffee shop. How safe are they?

WhiteHat Security says that: 'Cybercriminals are increasingly targeting mobile apps for attacks, due in part to lax security standards.' Some 85% of mobile apps WhiteHatSec tested were found to violate one or more of the Open Web Application Security Project (OWASP) Mobile Top 10. That makes mobile apps a gaping security hole. Yet, it's not hard to build secure mobile apps if your developers know what they're doing.

Penetration testing can spotlight vulnerabilities, if done with diligence. The hardest part is controlling how mobile and portable devices are used. BYOD is almost ubiquitous now. That makes it near impossible for IT teams to make sure that only approved apps from authorised sources are installed. Keeping patches up to date is another headache. Educating your users about security is essential here but isn't infallible.

Testing Times

Inexperience tends to show up in unexpected places. Not in how the software functions because it usually does what the customer wanted.

Inexperience shows up in non-functional requirements like performance, ease of use, scalability, reliability and more.

Other areas that can hold unpleasant surprises are the ability of new applications to integrate with your current systems or off-the-shelf applications you need to add later. If a new application is designed as a cloud service, the cloud provider's hosting security and the jurisdiction where your data is stored are critical checkpoints as well.

The bottom line is that building quality business applications relies on experienced, trained software engineers using proven processes. It depends on thorough acceptance testing, performance testing, load testing, cross platform testing, cross browser testing and penetration testing for security. There are no shortcuts.

I've focused on security here because it's a key issue for all organizations, and it's pretty clear that it pays to choose a software house that has both the necessary skills and the track record in software development and security.

A lot of our work turns on integrating various software modules – off-the-shelf and bespoke - with the systems customers have already deployed. This often includes the modification or design of APIs that allow disparate systems to talk to each other or share data or connect to external systems or cloud servers. This is a technically demanding area that requires special skills.

It comes down to choosing the best partner for your project, and that means making sure that their experience and skills profile is a close match for your needs.