Building Longevity Into Your Online Systems

WHY PLAN FOR LONGEVITY?

Your online presence is a major part—for some organizations, the only part—of how you interact with your users and stakeholders. Getting it right can be a major investment, involving months if not years of planning.

Designing for longevity will help to ensure that this investment will pay off, and will avoid the frustrations of expensive upgrades to keep up with technology, extensive re-designs to accommodate changing online habits, and annoyed users who have to re-learn how to interact with your organization when you are forced to roll out major changes for reasons that may not be apparent to them.

But the online world evolves rapidly, and change is inevitable. It is important to understand how and why things are changing, both to accommodate those changes that have already overtaken us, as well as to anticipate your future needs so that you do not get hit with unexpected costs and delays down the road.

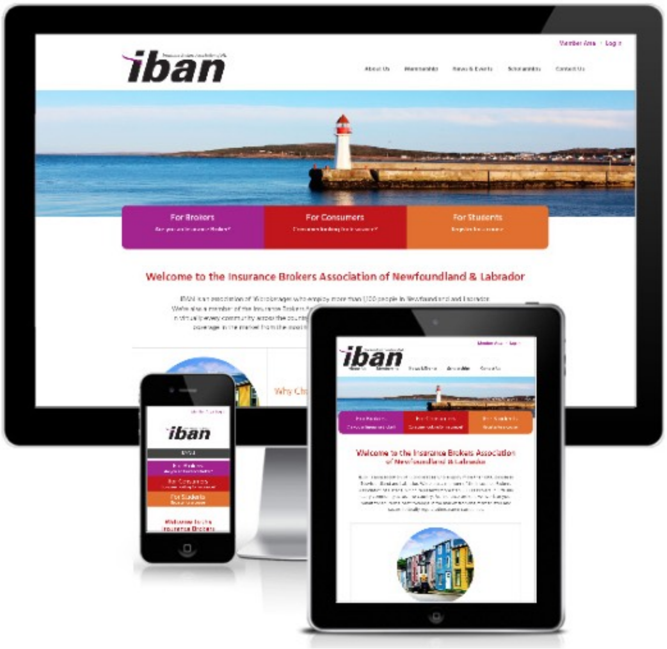
What issues have been driving online technology changes over the last 5-10 years?

The online world of 10 years ago was poised for change. The clunky and aging *IE6* browser had recently seen the first of a series of long overdue upgrades with *IE7*. The *Google Chrome* browser was about to be released. And the revolutionary iPhone had just been launched, which would change the mobile world forever. The changes that these and other developments brought to the online world were significant and sweeping.

New **online standards**, which had been held back by legacy browsers like IE6, could finally get some traction, which allowed for a rapid development cycle between web designers and browser developers as many new techniques became possible to deploy commercially. These standards have since stabilized, as technology has begun to catch up with long pent-up needs.

The **mobile revolution** has brought big changes to how we interact online through our phones and tablets. For years, designers had been gradually enlarging their designs to accommodate bigger computer displays, richer media, and higher-bandwidth connections. Now suddenly they had to accommodate pocket-sized screens, and visitors with spotty connections and limited data caps. Fortunately, new responsive design paradigms now allow us to design for multiple screen types simultaneously.

The rise of **mobile apps** offered an alternative to the web browser as a way to interact with organizations. And not just organizations—friends and colleagues as well. **Social media** exploded with the mobile revolution, creating new modes of interaction, new marketing channels, and new forms of analytics to measure performance.


iban
For Brokers
For Consumers
For Students
Welcome to the Insurance Brokers Association of Newfoundland & Labrador

The rise of mobile devices means that websites need to be designed for multiple display sizes simultaneously.

Software-as-a-service (SaaS) became an increasingly popular way to implement online services. No need to mess with complicated software installation and IT issues—just subscribe to a service online, login, and start working right away. But of course, that also leads to a pitfall—if the service shuts down unexpectedly, you can lose all of your data and your operations can grind to a halt.

Content management systems (CMS) became commodified—so ubiquitous and popular, that quite powerful systems were now available for no cost, or as SaaS solutions with cheap or even free service levels. These tools have rich ecosystem of plug-in extensions, and a large pool of experienced developers to draw from.

If you have had to go through an online redesign or redevelopment project in the last few years, you have probably had to take some or all of these factors into account in your planning.

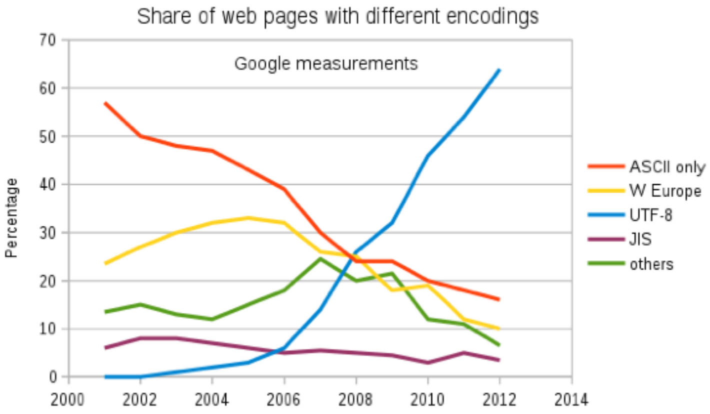
What issues continue to be commonly overlooked?

It is relatively easy to keep on top of hot topics like mobile design and social media, because they are high-profile, visual in nature, and easy for the layperson to grasp. However, there are other current trends that fly “below the radar” and do not get the attention they deserve.

Accessibility for the disabled is often overlooked. The desire to build a website that is exciting and visually appealing can often lead to design choices that are sub-optimal for visitors with visual, motor, or even auditory disabilities. For example, a reliance on audio-video content can be problematic for blind and deaf visitors. Popups, flyouts, carousels, and other animation effects can be troublesome for visitors with motor disabilities who may have problems tracking the movements and finding their way to simple hyperlinks. It is not uncommon for organizations to declare a desire to accommodate the disabled in their web design, and then make a succession of choices that prioritize flashiness for the fully-abled over that objective. But with the recent improvements and stabilization in web standards, it should be easier than ever to design with accessibility in mind.

Bandwidth usage and **page bloat** continue to be serious problems. Back in the days of dial-up connections, designers gave some thought to keeping their pages lean and fast, but broadband internet has given us a lot more freedom to be bold with our data. But the rise of mobile devices means that many of your visitors are once again on slower cellular connections with limited data caps, so we've come back to a time when light-weight pages are appreciated. Over-reliance on "heavy" media like video, high-resolution cosmetic imagery, and background tracking services that generate lots of network activity can really slow your site down and make it a frustrating experience for some visitors.

The Internet has global reach, and information can arrive on your website or be pushed out through your website in **various languages**. Current standards make it easy to support character sets like Unicode (UTF) that can handle virtually any language, and a good CMS will provide support for multiple languages in your regular content maintenance. This is important not just for organization with international reach, but also for Canadian organizations that need to provide official support for both English and French domestically.

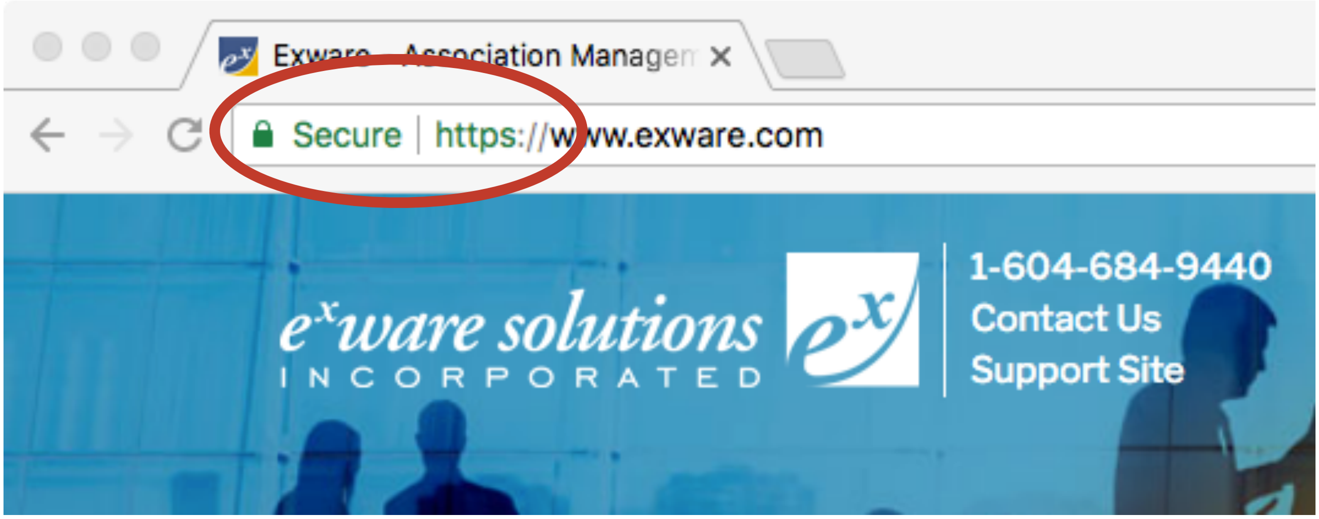


Rise of UTF encoding for multilingual support (Wikipedia)

Database breaches and **data theft** are an ongoing problem in online security. Few organizations give adequate thought to the consequences of data theft. If you ever get hacked, what sort of information could the hackers download from your online systems? Is there any sensitive financial information there, like credit card numbers? Is there enough personal information to allow for identity theft? Are passwords securely encrypted so that they cannot be used to attempt to crack other web sites? Are you using popular or off-the-shelf software tools or content management systems that have known security issues and hacks? Any system that collects or transmits personal data should be giving some thought to the consequences of that personal data being stolen and made public.

Mass-scale data theft is the most severe consequence of a failure in **privacy protection**, but there are other less dramatic ways you can inadvertently compromise your users' privacy. A full-scale hack can compromise the privacy of your entire database of users, but simply running without **SSL encryption*** can compromise them one at a time. The rise of public wifi access means that more and more often we are interacting with websites and online services through shared wireless access. Many users are unaware that anyone else in the same library, coffee shop, or airport lounge can, in principle, eavesdrop on their communications. For this reason, SSL encryption of all website communications is strongly recommended. Even with encrypted communications and encrypted

* SSL = secure sockets layer, a way of encrypting web communications. Also called secure HTTP, or HTTPS.



Are you using SSL (https)?

passwords, a weak **password policy** means that automated bots might still be able to simply guess your passwords and get into your website or email without any clever trickery.

Cloud computing has made it easier than ever to deploy servers on the internet, but the very nature of the cloud means that you have much less control over your privacy. Where are your servers really located? If you cannot say with any specificity, you may be in violation of laws that require personal information to be kept securely in certain legal jurisdictions to ensure it is handled appropriately. And with the increasing use of SaaS and online services that exchange data through APIs, it is getting increasingly difficult to understand exactly where your data is kept.

What are some current best practices you should be following?

If operating your own software and servers, choose tools and platforms with a proven history. Ensure that the intellectual property and licensing terms are generous to you in terms of how and where you are permitted to run the software. Open source applications and platforms like LAMP* are generally the most generous in this regard, and have a good chance of long-term maintainability and availability. Have a plan for regular IT maintenance and upgrades to ensure you do not accumulate security vulnerabilities that put you at risk. This is especially important when using popular CMS platforms that are the subject of regular hacking attempts.

* LAMP = Linux + Apache + MySQL + PHP/Python/Perl, a popular technology "stack" for web-based services.

Be careful about relying on SaaS solutions for mission-critical operations. You ultimately do not have control over the service delivery, and your suppliers can suddenly shut down or go out of business. Choose reputable providers, with a good history of service. Have a back-up plan if they suddenly shut down. Ensure that you can obtain backups of your important data so that you can plan for a transition in the event of a shutdown.

Use up-to-date web standards, particularly, HTML5, CSS3, UTF-8, and SSL (https).

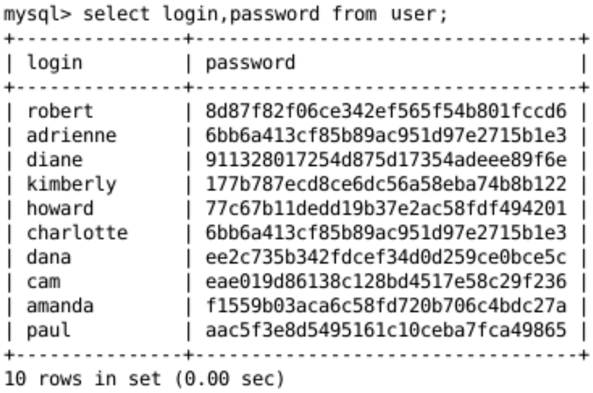
Use responsive design to support your mobile devices, in conjunction with a **responsive framework** such as *Bootstrap* or *Foundation*. In your content layout, beware of the urge to lay things out in multiple columns, as that creates problems on small screens when columns cannot be reflowed due to the limited space available. Even when using a good responsive framework, you need to use special techniques so that your content appears correctly on different types of devices, and these techniques are not always easy for the layperson to understand.

A good framework properly used will also help with your accessibility design, and will provide cues and aids for disability readers to deal with your site navigation, clickable controls, animations, and core content.

Be careful about investing in native mobile apps. Native apps are platform-specific, so they have to be developed separately for each platform you want to support. For example, once for iOS (iPhone), and again for Android. If you want broad, multi-platform support, that means extra development costs. Additionally, deployment of native apps can be slow, as apps need to go through an approval pipeline before they become available for download. A common way to deal with this issue is to use a web view (a web page wrapped up as an app) to present your tools and data to the user. That means that updates to your web presence can automatically be picked up and reflected in your app. Even simpler is to simply use a mobile website (or your responsive mobile view of your regular website) instead of investing in native app development.

When possible, outsource high-liability sub-services like **payment processing** to reputable providers. It is getting easier and more reliable to have well-integrated payment processing without you ever needing to take on the liability of handling the customer's credit card information.

Encrypt your communications whenever possible. Use SSL to protect all communications to and from your website, using either traditional security certificates, or a more cutting-edge alternative like *Let's Encrypt*. Further encrypt sensitive information that you store in your database, especially passwords, which often get re-used on multiple websites.



```
mysql> select login,password from user;
+---------------+----------------------------------+
| login         | password                         |
+---------------+----------------------------------+
| robert        | 8d87f82f06ce342ef565f54b801fccd6 |
| adrienne      | 6bb6a413cf85b89ac951d97e2715b1e3 |
| diane         | 911328017254d875d17354adeee89f6e |
| kimberly      | 177b787ecd8ce6dc56a58eba74b8b122 |
| howard        | 77c67b11dedd19b37e2ac58fdf494201 |
| charlotte     | 6bb6a413cf85b89ac951d97e2715b1e3 |
| dana          | ee2c735b342fdcef34d0d259ce0bce5c |
| cam           | eae019d86138c128bd4517e58c29f236 |
| amanda        | f1559b03aca6c58fd720b706c4bdc27a |
| paul          | aac5f3e8d5495161c10ceba7fca49865 |
+---------------+----------------------------------+
10 rows in set (0.00 sec)
```

Even if hackers get access to your low-level database, sensitive information like passwords should only be visible in encrypted form.

What upcoming issues are likely to become more significant in coming years?

The future is uncertain, but nevertheless there are looming issues that are either recent technological advances or hot trends that might yet develop into significant areas of development.

Cloud computing services are getting better at providing regionally restricted cloud domains, to better deal with privacy regulations like PIPPA and PIPEDA. For instance, *Amazon* has announced Canada-only availability zones in their cloud services, and if these prove reliable, we can expect more migrations to cloud hosting.

Content delivery networks (CDNs) are becoming increasingly important when delivering content to a geographically distributed audience. These services are typically used by publishers, but CDN services are becoming easier to deploy for other types of websites. As with cloud computing, CDNs can distribute your data and content geographically, and you will need to be aware of which data is on the CDN and where it is actually situated to ensure you stay within privacy regulations. Similar concerns apply to mobile content accelerators like *Google AMP*.

New mobile technologies are making it easier to build mobile websites that act and feel like native apps. **Progressive web apps** attempt to use advanced browser capabilities to provide app-like capabilities (such as push notifications, or offline functionality) when browsers allow it, but degrade gracefully to simpler website behaviours when they don't. This lets you embrace bleeding-edge technologies before they are widely available, which makes it much easier to plan for the future.

Ultra-high-resolution (“**retina**”) displays are becoming more common on both mobile and desktop devices. Standard-resolution web designs can appear blurry or lower-quality on these devices. As the popularity of these devices increases, there will be more pressure for organizations to update their designs to accommodate them. But since higher-resolution imagery also makes for larger bandwidth usage, this also runs contrary to our need to keep the mobile experience lean and fast. Designers and browser developers are working out new techniques to allow for deployment of retina content without adversely impacting mobile download speeds and data caps. As these techniques become more polished and standardized, we can expect more pressure for widespread adoption.

New **payment processing** technologies (like *Square*, *Stripe*, and *Apple Pay*) are making it easier to support advanced electronic payment services like on-site payments, automatic renewals, recurring payment plans, micro-payments, and refunds, without taking on the liabilities and risks of holding the customer’s credit card data. As sellers, we can expect more competition to arise in these next-generation payment services with more options for how to bill our customers, and as buyers we can expect newer and easier ways to pay smaller amounts, but more often, for online services.

Machine learning and advanced analytics are making it possible to mine your own data to identify patterns and business opportunities that are not obvious. But as these methods grow in popularity, the incentives to collect and track more information about your users will increase commensurately, so that you have more data to mine. But this will in turn create more privacy risks as you increase the information you hold about your user's demographics and online habits. It may be necessary to develop policies for clearing or anonymizing old data to reduce your future risk.

Machine learning can also be turned against you. **Malware** and **bots** are constantly evolving to exploit security defects and take advantage of misplaced trust in users. In the past, bots have taken the form of simple crawlers that go through your site snooping for things of interest, but with the rise of social media, they are increasingly being designed to mimic humans, create false trust, and engage with communities as part of widespread influence campaigns. It will be necessary to maintain constant vigilance to ensure that your own users' trust does not get eroded by pointless postings from robots, or phishing attacks that specifically target your services.

Finally, we can expect social media to continue its rapid evolution. Major social media services now have fully global reach, but that also means they attract unprecedented attention from the aforementioned bots and influence campaigns, which often have dubious intentions. We can expect rapid changes as this battle for attention and trust plays out on these social services, and as users' patience for these online shenanigans waxes and wanes.

How we converse online has never stopped evolving, and shows no signs of stabilizing any time soon. We have gone through e-mail, listservs, chatrooms, forums, blogs, Facebook, Twitter, Slack, and many more. Finding the right way to converse with your community will continue to be a delicate balance of old and new for the foreseeable future.

SUMMARY – DESIGNING FOR LONGEVITY CHECKLIST

A quick overview of some of the major issues affecting the longevity of online and web-based systems.

SOFTWARE TECHNOLOGIES

□ Are you using up-to-date web standards?

□ Does your software have open licensing terms?

□ Do you have IT support to keep your software updated and secure?

□ Do your SaaS applications allow you to recover/download your data?

□ Do you have a rapid recovery plan if your your SaaS applications shut down?

WEB DESIGN

□ Are you designing responsively for both desktop and mobile devices?

□ Are you using a responsive design framework?

□ Is your design sensitive to cellular data speeds and bandwidth caps?

□ Do you have a mobile app or app-like web experience?

□ Are you designing accessibly for people with visual, auditory, or mobility issues?

□ Are you designing for ultra-high resolution (retina) devices? Do you need to?

SECURITY

□ Are you using SSL?

□ Are you further encrypting sensitive personal information, including passwords?

□ Do you have a published privacy policy, is it up to date, and are you adhering to it?

□ Are you collecting an appropriate amount of personal information?

□ Is your data hosted/stored in an appropriate legal jurisdiction?

□ Is your payment processing/credit card handling appropriate for the types of payments you handle?