Keep Pace With Innovative and Secure Technology

SmartVault

Introduction

If you tune into the news from the tech world, you can't help but find a recurring theme. Supposed cutting-edge software company announces a data breach. They say it's not too bad.

It turns out to be far worse than they initially said. There is a short burst of outrage from consumers, competitors, bloggers, politicians. Legislation is promised. Software moguls are shamed. Then everyone forgets about it and moves on to the next story.

Bad news fatigue is real. People are hopelessly tired of the constant barrage of news about companies' data breaches, hacks, and unethical behavior. Add to that the propensity of tech content creators to dub every new technology as the next big thing, and you have a veritable maze of misinformation and misdirection.

It's a shame because most of us want to stay up-to-date on the latest technology and keep our data safe. However, it is not easy to filter the sensationalist journalism that will keep you afraid from the actionable information that will keep you safe.

This eBook will explore ways to keep pace with secure technology without wasting too much time - and without losing your mind.

What the news gets right

The news snippets are right about two things.

The first thing is that ***no one is safe from data breaches.*** There's an army of malicious agents working overtime, looking for exploits they can monetize. It's tempting to think you are safe simply because you're under the radar - but it doesn't work like that. While high-profile breaches like the one that happened to Facebook in 2021 are the most widely broadcasted, small businesses are just as likely to fall prey to attackers.

A 2022 report finds that 81% of ransomware attacks target small businesses. While the payday for attackers is much smaller when targeting a small company compared to a major corporation, the upside is that it's much easier - most small businesses either don't bother with cybersecurity protocols, or they don't stay up-to-date.

The second thing the news gets right is that ***tech evolves very quickly.*** Every day, there are developments that may or may not change the world - or, at the very least, change an industry. In the realm of personal computing and internet oddities, you may find it easier to tune out and stick to what you know. But in the world of business security, apathy can be dangerous.

For these two reasons, it's paramount to keep pace with technological advances, particularly in the area of security. The first thing to focus on is filtering out the noise - and there is plenty to filter out.

Filtering out the noise

Once we start tuning out of stories using the filters above, we naturally gravitate towards better content and creators.

Individual content creators aiming to build a community are often better sources of information than traditional media outlets that aim to increase their ad revenue. But, of course, there are plenty of disreputable content creators out there as well.

Take the web3/crypto space, for example. Many creators are selling their own NFTs and pushing altcoins after investing in them. Even many big names, such as Chris Dixon, have a clear upside from you investing in crypto. If you're interested in understanding the technology and its implications, following creators such as Nader Dabit will better serve you.

The same applies to other areas of technology. Quantum computing is a potential game-changer for many industries, but filtering through the hype is near impossible. Finding out whether you need to prepare your business for upcoming changes in any way - and how - is a daunting task. When it comes to such innovative technology, it can be appealing to follow academics who are sharing cutting-edge resources that may not be widely available yet. For example, Aziza Suleymanzade has been sharing some excellent insights into quantum computing.

Bruce Schneier is a great focal point if you want no nonsense updates on security.

Generally speaking, if you join social media, what you should be looking for are technical experts who explain the implications of technological advances. Steer clear of anyone invested in recruiting users for a specific technology. Especially stay away from self-styled ''evangelists'' for tech with unclear purpose and suspicious security standards.

Knowing who to follow

To start, ***filter out exotic, one-of-a-kind stories that aren't repeatable in the real world***. When a breach happens in a bank's internal software, and rogue employees make off with a billion dollars, it makes for sensational news. However, it does not make for an actionable lesson for you (unless you happen to be the CTO of a major bank).

Another thing to ***be wary of are stories that have a fearmongering tone and then end by trying to sell an expensive solution.*** This is likely a thinly veiled ad. There are plenty of these going around, particularly in unregulated online publications. Before making any decisions based on such stories, cross-reference them with more reputable sources. If a report claims a catastrophic calamity happened, but no other sources confirm it, then it didn't happen.

You do not, generally speaking, need to invest in expensive software to protect yourself. ***Being safe is usually a matter of making a critical update here and a small purchase there, but, primarily, it is a matter of being vigilant and resourceful.***

If a story gets political, extract the technical details and focus on those. Learning about a security update usually takes less than an hour. Keeping track of congressional hearings and legislative changes, on the other hand, can take months.

Last but not least, ignore anything that presents a technical issue as the end of the world. Whatever happens, the world will still be here tomorrow, unchanged for the average small business. Stories that claim otherwise are sensationalist and devoid of any real value to the reader/viewer.

Cross-reference everything

It is improbable for important news to only appear in one publication (unless the author is the hacker that uncovered a security hole and is nice enough to write about it). Sure, journalists find the occasional exclusive scoop, but in tech, news travels fast, and others will soon be vying to either amplify the information or discredit it.

When considering multiple news sources, the crucial thing is that they are uncorrelated. You gain nothing by reading four sources if three of them simply paraphrased the opinion of the fourth. Compare rival publications and rival content creators from different countries if possible.

In the words of Daniel Kahneman, the Nobel Prize winning pioneer of behavioral economics: *"To derive the most useful information from multiple sources of evidence, you should always try to make these sources independent of each other."*

Nothing beats live events

If you're interested in having a conversation instead of simply consuming information, nothing beats face-to face interactions.

Plenty of tech conferences worldwide are returning to their pre-pandemic ways. Some are focused on cybersecurity, like RSA (San Francisco) and Infosecurity Europe (London).

At conferences, you are not relegated to the role of a passive spectator - you can often take part, ask questions of presenters, and mingle with industry heavyweights.

Many companies use conferences to make announcements about breakthrough technologies and new applications of existing tech. Hearing this sort of news from the horse's mouth is much more reliable than having it filtered through media outlets. Add to that the very real advantage of being able to take part in the conversation and you have a very strong case for attending a few major conferences per year.

Asking good questions

It is crucial to ask broad questions whenever a technological breakthrough happens.

What is driving change in this area? What is behind it? What is the context? Who are the major players?

Context is important. Be especially vigilant if geopolitics plays any role whatsoever in the developments. A security update published by a government agency in response to a foreign threat is likely to be shrouded in secrecy as much as the threat itself. You will never really know what you're getting or what danger you're supposed to be averting.

On the other hand, white hat hackers and security startups are more than happy to be open about both the problem and the solution, and it's much easier to make an informed decision on the matter.

Managing new information

So, you've filtered the information from various sources. You've checked the reliability and understand the events in the broader context. Now what?

Gathering information is not enough. We must analyze the data and categorize it. In the case of data breaches, we should estimate our vulnerability to them.

In order to keep your company's tech stack up-to-date and secure, it is imperative to react promptly to critical developments. To do this, first, we separate all the new information in order of importance. A good set of categories to use:

- Critical
- Important
- Nice-to-have
- Unimportant/luxury

Critical items are the ones that can affect the security of your data immediately. These are data breaches that your software is vulnerable to. These must be dealt with immediately, whether by delegating to your IT experts or implementing a ready-made solution from a reputable vendor.

Essential items are the ones that can affect your company's relevance and competitiveness in the long run. This includes any new software or hardware that can be used in your industry to cut costs or increase profits.

Nice-to-have items are the ones that help nurture a culture of innovation, boost your reputation as a cutting edge company, enhance employee morale, or otherwise improve the overall atmosphere surrounding your organization.

Unimportant/luxury items are the ones that are best left alone - the sort that can help a founder's ego but have no positive effect on the company's bottom line. Think of technology that is way too advanced and redundant within your industry. Times change, however, so it's not an insufficient exercise to log such ideas somewhere and revisit them occasionally to keep an eye on any updates.

Humility is a virtue

Making quick decisions is often required of business leaders. However, it can also be dangerous.

If you're unsure how to handle a piece of information or correlate it with other data points, don't hesitate to consult an expert. If you have colleagues or employees who are known to keep track of new tech, a quick brainstorming session can be the difference between a great decision and a disastrous one.

Bringing in outside help can also be justified if you assess that your company doesn't have the resources to manage the new developments effectively.

Most companies discuss emerging technology by having a meeting where one person gives a presentation, and then everyone else is invited to comment. A better way to start a constructive discussion is to have everyone involved write down their opinion beforehand. That removes the effect of a presentation: most people are inclined to agree with the speaker for fear of looking silly or misinformed. If everyone is asked to do their own research before the meeting, the discussion will be much more open.

Diversity of opinion is good for everyone. Make your meetings a positive-sum game, and they will never feel like a waste of time.

Summary

Tune out the noise, focus on what matters, and listen to knowledgeable voices. Those are, in short, the three tenets of keeping pace with innovative and secure technology

Weaving through the congested traffic of tech content can be overwhelming. Many give up. Others are seduced by the tabloid nature of many tech writers and podcasters.

Some fall prey to scam artists selling digital snake oil. Some become content creators in this space themselves, propagating whatever they think is true - or whatever they believe will generate search engine traffic.

Few do it right, which is why so many small businesses are left exposed every time there's a new kind of breach or a new vulnerability. Many are still caught off-guard by technological advances that render their services outdated and their business model obsolete.

Tune out the noise, focus on what matters, and listen to knowledgeable voices. Those are, in short, the three tenets of keeping pace with innovative and secure technology.

Ready to see SmartVault in action?

Schedule a 15-minute demo with one of our document management experts or sign-up for a free 14-day trial today!

SCHEDULE A DEMO **START YOUR TRIAL**

SmartVault

www.smartvault.com