We Take Security Seriously

This is a phrase uttered by many businesses that want to build trust with their partners and customers or that need to rebuild confidence in the wake of a breach. But what does taking security seriously actually look like - both for customers and providers?

Table of Contents

1. Introduction

Whether you're setting up a new enterprise security department, or maintaining an existing one, you've probably been asked if you are taking security seriously enough. All too often, the knee-jerk response is to state that without a shadow of doubt, you take security very seriously. But, what does that translate to in real life?

I've worked in security my entire professional career in different capacities: as an IT security administrator, a consultant, an industry analyst, and now a security advocate - and even I couldn't give myself a satisfactory answer to this question.

Wanting to scratch beneath the surface, the intention of this report is to throw out lip-service and get to the heart of the matter by attempting to quantify how a person can demonstrate that they take security seriously?

2. Outlining the Problem

2.1 It Depends

When someone says they take something seriously – how do you measure their level of seriousness?

We're dealing here with an imperfect science. You can't measure intent or goodwill, so there needs to be some other form of measurement.

Unfortunately, the information security space, or cybersecurity as it is often referred to these days, is an area where gaining consensus is not as easy a task as one would hope.

Even the experts can't agree on some of the most fundamental of controls, such as whether or not a password should expire on a regular basis, or how long or complex they need to be.

Instead, what we see in reality is that for any question asked, the response generally needs to be contextualised with, "it depends". What this actually means is that security controls will have to be in line with the risks. Understanding a business, the threats it faces, and its ability or desire to defend against those threats will help formulate the answer.

In June 2018, a Polish charity had to cough up 2,700 Polish zloty because someone stole the tracker from a stork it was tracking and used the SIM card to rack up hours of phone calls.

The environmental EcoLogic Group had placed a tracker on the back of a white stork last year to track the bird's migratory habits. It travelled some 3,700 miles (6,000km) and was traced to the Blue Nile Valley in eastern Sudan before the charity lost contact.

Somebody found the tracker in Sudan, removed the SIM card and put it in their own phone, where they then racked up 20 hours' worth of phone calls, which Ecologic had to pay.

Do you think the charity had factored such a situation into their threat model? Not likely.

2.2 Hello Compliance My Old Friend

Many companies will say that they are taking security seriously because they have achieved some type of compliance. But does compliance alone equate to taking security seriously? After all, it does take time, effort, and resources to achieve any sort of compliance.

The reality shows that many companies have been compliant with certain standards, yet still suffered breaches. One of the problems is that when applied in isolation, it only addresses a small portion of the overall security requirements.

For example, if a company is evaluating its application security, the scope is usually limited to the session, presentation, and application layers. If the operating system and network infrastructure are out of scope, then any misconfiguration can impact the application security. Hence, to take security seriously, one has to look at the big picture and not do the bare minimum to tick the box.

That being said, for many companies, compliance is a good driver. It can also help to attain a reasonable minimum baseline when it comes to security. However, these standards need to be applied with a certain level of understanding of the larger context, which is often not part of the picture.

As Simon Sinek popularized in his TED talk, people are often good at explaining what they do, or how they do it. But they tend to be poor at explaining why they do it.

We often see that compliance is viewed through a similar lens; companies may be aware of what they are doing, and how they are doing it, but frequently miss the critical "why". However, the why isn't always straightforward to understand, which is why it requires considerably more thought than the "what" or "how" components.

2.3 A Defensible Position

If you've ever embarked on a fitness journey to get a 6-pack, you'll likely have read that abs are made in the kitchen, not the gym. Putting an hour or two of effort at the gym is the easy part, but it's having self-control and discipline for the remaining 22-23 hours that makes all the difference.

The same concept could be applied to security. Being serious about security isn't necessarily based on the toolset or the process. It isn't even about preventing incidents or breaches altogether. Rather, being serious about security is more like a mindset, or a way of life.

So it boils down to a matter of risk. Can the provider give a defensible position as to whether they are actually taking things seriously or not?

Extending the food analogy by borrowing from Wendy Nather, most companies end up practicing what she refers to as, "Cheeseburger risk management" - in which companies accrue security risks in the same manner a person will eat cheeseburgers (or other unhealthy food) over a period of years because they don't have an immediate ill effect - until the cumulative effect results in a heart attack.

3. Bring Out The Experts

> *"A business with an online presence (has a website and transacts or stores data, payments) states that 'it takes security seriously' – as a security expert, what would it take for you to believe that statement?"*

I posed this question to a number of security professionals. The question was intentionally vague – there wasn't intended to be any steering or biasing – but I asked it as a way to try and gauge how experts view the statement and what it actually means to them.

The vague nature of the question generated a list of controls, but also generated a lot of thought-provoking commentary. Listing all the commentary is beyond the scope of this report, but some select quotes have been provided throughout.

> *"I think if you start with an assumption of their posture, you then have a bunch of possible negative indicators.*
> *So an org wanting to win my trust needs to remove as many visible negative indicators as possible.*
>
> *A big, big step (if it's a small site) is for them to realize that they can't (easily) prove to me that they are secure. Instead, they can convince me to transact anyway by borrowing trust (i.e. pay through Stripe...we don't keep your credit card at all).*
>
> *People need to realize that customer data is like a kind of toxic asset. A small company that wants me to transact needs to signal that they understand this." - Haroon Meer*

3.1 The Controls

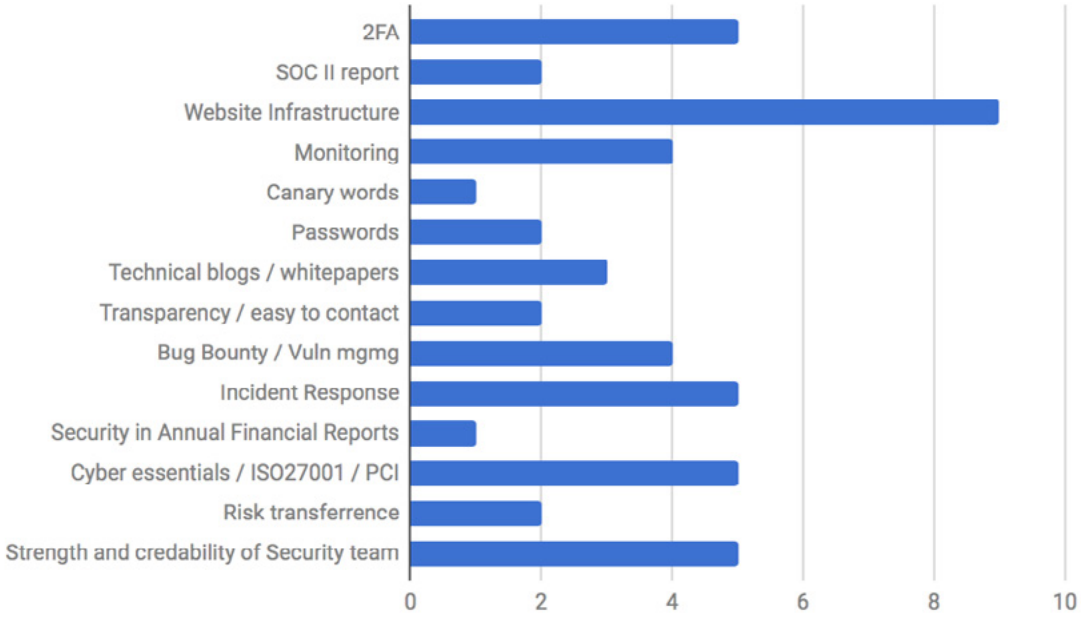
There were many similar controls that various experts listed; for simplicity, these were grouped together into 14 separate controls.

- 2FA
- SOC II report
- Infrastructure stuff - Padlock / SSL / TLS / CDN / Sec headers (score well) CSP in block mode
- Monitoring - Notification of changes (new device, profile pwd etc)
- Canary words in privacy statements
- Password strength / storage
- Technical blogs / whitepapers
- Transparent security / transparency reports/ easy to contact
- Bug bounty / vuln disclosure and management
- Incident response / communicating with all parties
- Putting security section in annual financial reports
- Cyber essentials / ISO27001 / PCI
- Transferring risk e.g. 3rd party payment processors
- Strength and credibility of Security team

3.2 How many times did each of these controls come up?

As you'd expect, these controls focused on observable security measures. Technical controls relating to a website's infrastructure came up the most often. The website is, after all, the window into an organization, and one can draw

some conclusions as to how well a company handles security by how well it secures its website.



In the second most popular group, two-factor authentication and compliance certifications such as ISO27001 and PCI DSS were among the technical and measurable controls.

Incident response capabilities were also mentioned with the same frequency, although this is more of a reactive control that can only really be measured after an incident. There are many facets to this that would include how quickly the incident was discovered, the quality of communication, and how quickly and effectively the issue was resolved.

Interestingly, this second group also included the strength and credibility of the security team. There is no general consensus on how the strength or credibility of the security team could be measured and would be biased based on how one feels about particular individuals. Still, it shows that for security leaders, building individual credibility, i.e. by sharing research and presenting at conferences, can improve how their company is perceived in terms of security.

Having good monitoring, vulnerability management a bug bounty process were cited as the third most popular set of controls. This is particularly interesting because these are detective and response controls.

It's worth noting that none of the security professionals that participated cited any common preventative controls such as firewalls, anti-virus, DLP, etc. This is most likely because those are considered primary controls that every organization should have in place anyway; having them in place is not, therefore, a measure of taking security seriously[1].

Having good monitoring (to detect a breach) and a good vulnerability management plan, preferably tied in with a bug bounty program, also gave confidence that a company had relatively mature security processes and knew what they were doing.

> ***Firstly, never say that [we take security seriously]. It's the first thing that people say after they've been breached, and has turned into the infosec equivalent of "it's not you, it's me" - Find something better, more meaningful, and most contextual to your company.***

[1]It is worth referencing the research papers by Wendy Nather on the topics of "The security poverty line", and "The real cost of security". The latter in particular surveyed experts on what would be a minimum baseline of security controls in which the common set of security tools were widely listed such as firewalls, SIEM, and so forth. It would be useful for the reader to reference those for background. Making this report an unofficial third, in a trilogy of sorts.

Re: believing that statement - One can never know how seriously a company takes security, so it comes down to relying on proxy indicators of security maturity.

One such indicator is CSP in block-mode. Effective, and a total pain in the ass to implement. If it's working, someone in the building actually cares about my data. There are many other indicators, but currently it's left to either the hacker-managers who can determine it themselves, or the VRMs who charge for the info.

Another is the presence of a vulnerability disclosure or bug bounty program, and stats around both their time to triage and remediate, and the level of reward they are prepared to offer... Higher rewards = more badass. - Casey Ellis

3.3 Ease of Implementation

Now that we have a list of critical controls, it would be disingenuous to simply say, "go forth and implement". We still need a way to establish just how practical it is to implement these controls.

As a customer, I don't trust anyone who says it. But certain things improve my confidence: 2FA, TLS, third-party certification (PCI, ISO, etc).

B2B, I run vendor risk assessments and ask for their latest penetration testing report.

Key things I look for are a running security program, vulnerability management, monitoring program, incident management. – Wolf Goerlich

The ease of implementation is something that probably needs to be discussed more when dispensing security wisdom. Knowing what to do is one thing; but going about actually doing it can be a very different scenario. There are many security controls that are often labelled as being 'basic' – which is why I prefer the term 'fundamental'. Much like in construction, a solid foundation is a fundamental part of ensuring the integrity of the building, but it is not necessarily a trivial task to accomplish this.

To gain a better understanding of the ease of implementation, a wider net was cast to get insights from a broader range of professionals. A survey was shared on Twitter where 54 respondents participated. Due to the inherent limitations of a survey, and not wanting to make the survey cumbersome, not all controls were listed. The only ones that were included were those related to the ease of implementation:

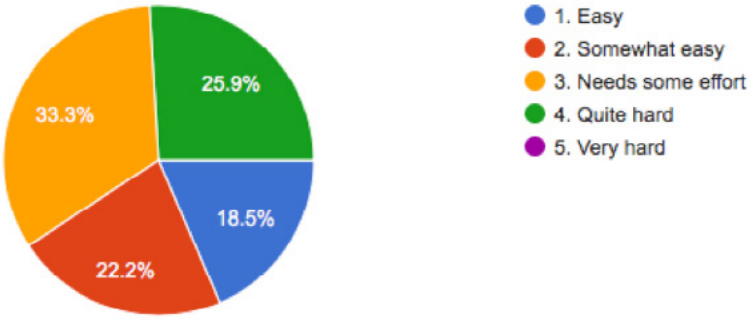
- Two-factor authentication (2FA)
- Monitoring
- Passwords
- Technical blogs / whitepapers
- Bug bounty / VM
- ISO 27001 / PCI DSS certification
- Incident response

Opinions on how easy it is to implement a control turned out to be very split. But this is not all too surprising as enterprises vary greatly in how they are setup, so implementing technical controls can also vary and are heavily biased by the respondent's personal experiences. For example, two-factor authentication may be easy for a company that is using cloud-services such as O365, for which it's a simple case of enabling the feature; but, if legacy systems are in place, it may not be so straightforward to implement.

Then there are the non-technical measures to consider. Perhaps enabling 2FA could be easy from a technical perspective, but a company's management or executives don't want it enabled because of the cost or inconvenience associated with it. This will obviously make it more difficult to implement.

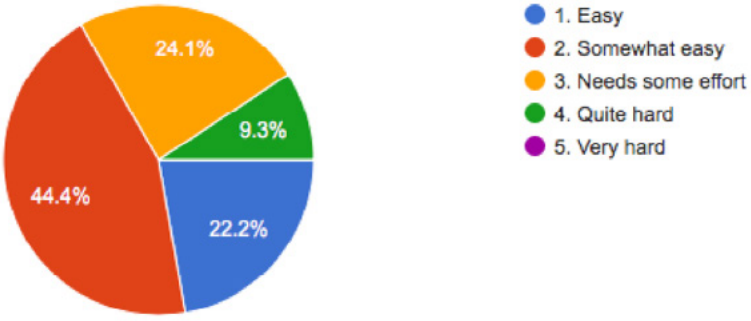
Two-factor authentication

54 responses



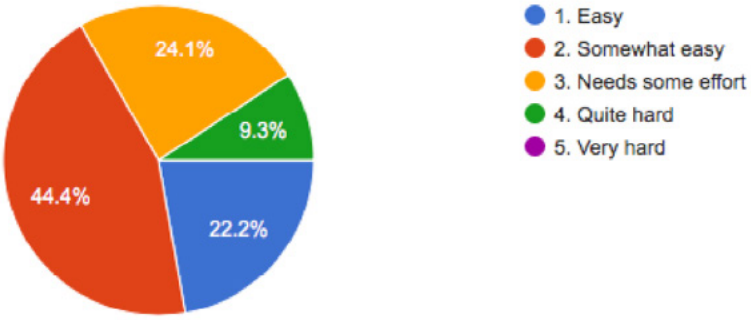
Visible website security (SSL, TLS, CDN, Sec headers, CSP...)

54 responses



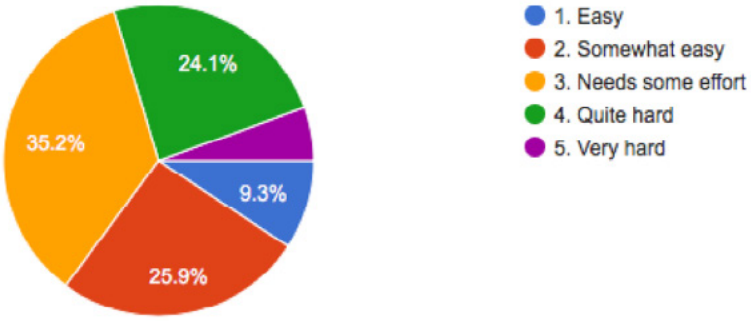
Visible website security (SSL, TLS, CDN, Sec headers, CSP...)

54 responses



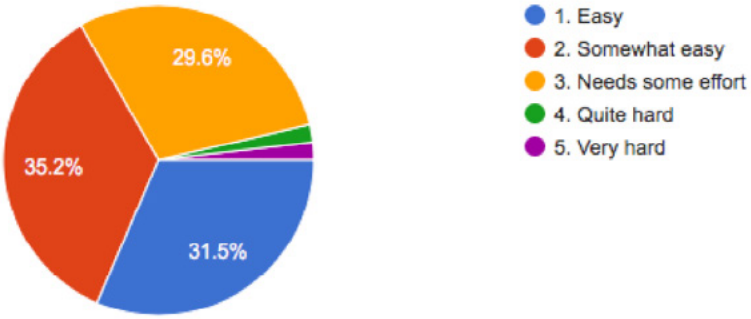
Monitoring controls (e.g. notify customers when password is changed, someone logged on, any settings changed, suspicious account activity etc).

54 responses



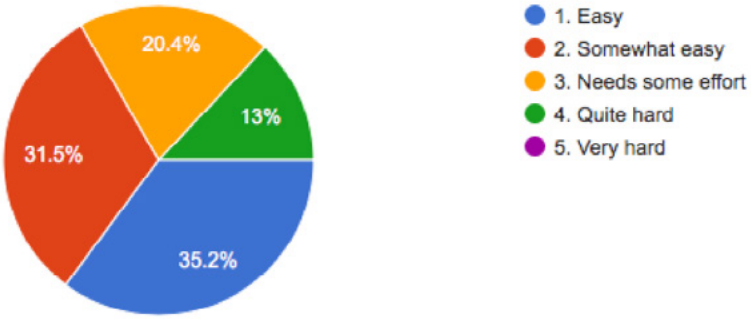
Good password policies, enforcing strong passwords and storing securely.

54 responses



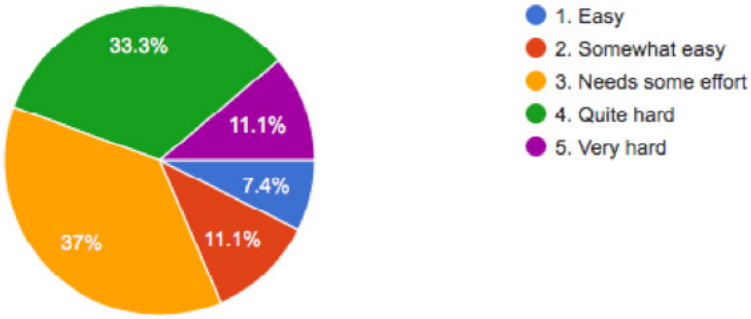
Making technical blogs and white papers available

54 responses



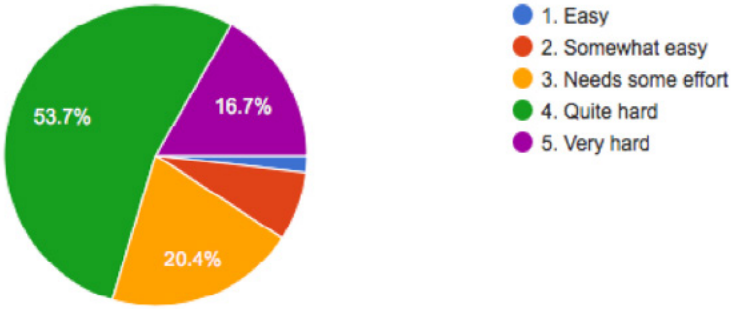
Having bug bounty / vulnerability management

54 responses



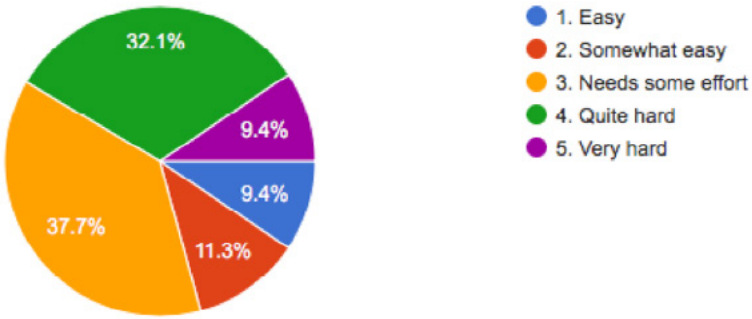
Good incident response

54 responses



Being certified (ISO27001, PCI, cyber essentials etc)

53 responses



I would be looking for many things including:

1. How public are they? is their infosec team public – do they make public statements? Can B2B customers talk to their infosec team?

2. Does their infosec team have any weight in company strategy?If not how seriously do they really take infosec?

3. How do they react and respond to infosec incidents? Is it clearly and confidently with the infosec team, comms and business ops acting as one?

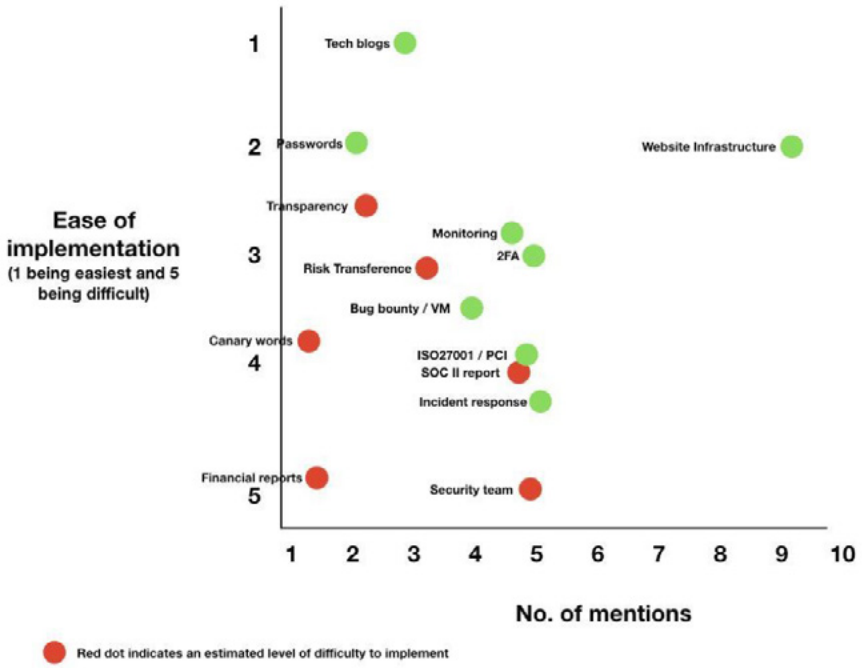
4. How do they react to vulnerabilities? Publicly thank and work with researchers or threaten to sue them?

5. Does their application / service have security baked in ie does it list login activity for example? Do they support 2FA? Of course all of this point depends on the relative risk - Quentyn Taylor

3.4 Frequency vs Ease of Implementation

Now that we have a base set of controls that come up frequently, and we have a general consensus on how easy it is to implement these controls - let's map them against each other.

The below chart shows the frequency of the controls as mentioned by the first group mapped against the survey for ease of implementation (taking the most popular response). Note that the green dots represent those responses which were from the survey, while the red dots are assumed difficulty levels by the author. As mentioned earlier, the ease of implementation will vary depending on personal experience, the technology used, and the overall organization.



From this, we can infer that having a secure website is one of the most heavily weighted elements by the majority of professionals, and is also broadly considered to be not overly onerous to implement. Therefore, it would represent the greatest return on investment for a company.

Publishing technical blogs or similar useful content was considered to be the easiest of tasks to achieve, and publishing such content can also help to raise the profile and visibility of the security team overall. So while recruiting an all-star security team may be difficult for most companies, consistently sharing valuable information can help overcome the hurdle by creating credible experts within the company.

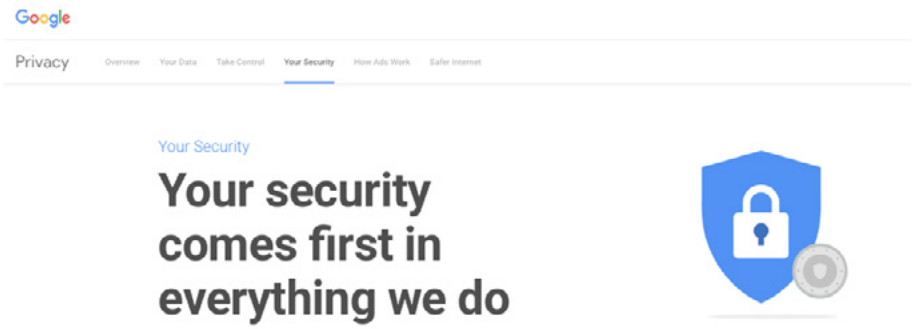
It would take the public assertion of a well-known person in the security community — An attestation that the vendor's security posture is high. - Jackie Stokes

4. Lay of the Land

Let's scour the internet and take a look at some common providers and see what they say about taking security seriously. Most of the large companies usually have public resources available that we can analyze.

> *I guess the first thing is like most people I tend to trust large, well-known companies.*
>
> *So I'd expect to either see a large organization that *probably* knows how to do its own payment processing, or an external payment processor like PayPal that knows what it's doing.*
>
> *Entering credit card details on a domain you don't know is always a bit of a risk.*
>
> *I guess on the technical side, PCI is pretty common as standards go in that it is quite strict. VISA doesn't like having to pay out for breaches themselves and hates even paying to investigate them.*
>
> *If you're trying to look externally - I guess looking at their job adverts might be enlightening. Do they pay market rate? Do they employ specialized security folk? - Chris Doman*

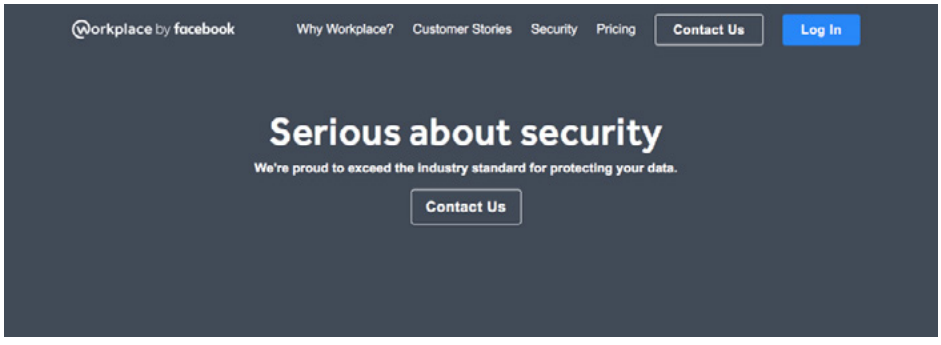
4.1 Google



Google talks extensively about how it takes security seriously. Some key features listed are:

- Encryption of data in transit
- Resilience with multiple data centers
- Continuous monitoring and threat detection controls
- Tips and advice for users to stay secure online
- Bug bounty
- Transparency reports
- Assurances that it doesn't sell user data or provide direct access to governments

4.2 Workplace by Facebook



Workplace by Facebook doesn't beat around the bush by declaring how seriously it takes security.

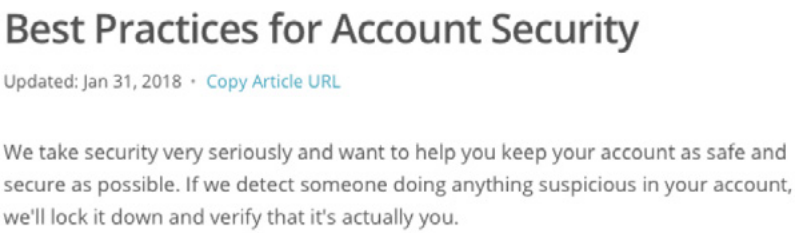
Its key points start with compliance,

- ISO 27001, SOC2, SOC3, EU/US Privacy Shield
- Principles of trust
- Encryption
- Physical security of data center
- Threat intelligence and threat detection
- Incident response
- Continuous risk assessment
- Security conferences
- Security tools such as osquery and ThreatExchange
- Full source code reviews
- Penetration tests
- Independent third-party audits

4.3 MailChimp

MailChimp also states clearly that it takes security seriously. It has several security articles in its knowledge base.

There are two indicators of this that they specifically mention, one being their internal threat detection capabilities to block any suspicious activity on user accounts, and the second is offering 2FA and security questions to authenticate users.



Best Practices for Account Security

Updated: Jan 31, 2018 · Copy Article URL

We take security very seriously and want to help you keep your account as safe and secure as possible. If we detect someone doing anything suspicious in your account, we'll lock it down and verify that it's actually you.

MailChimp offers a 10% discount to users who set up 2FA at login.

Set Up a Two-Factor Authentication App at Login

Updated: Jan 31, 2018 · Copy Article URL

Set up two-factor authentication to keep your account extra secure, and get a MailChimp discount. Two-factor authentication means that you'll need two forms of identification to log into your MailChimp account: your login credentials, and a unique passcode generated by a two-factor authentication app.

Because we feel so strongly about security, we offer a 10% discount for MailChimp accounts where all Owner and Admin logins have two-factor authentication set up. (Ad campaigns are not eligible for this discount.) Two-factor authentication adds an extra step to your MailChimp login process, but the security benefits make it worthwhile.

In this article, you'll learn how to set up and use two-factor authentication with an authenticator app, set requirements for other account users, and disconnect two-factor authentication.

MailChimp has a rather detailed security page which explains some of its security controls. Some of these are:

- Data center security
- Backups
- Application security – password hashing, SSL, brute force prevention, and penetration tests
- Mobile app security
- Internal security
- Staff training, including “the Art of Deception” being required reading
- Suspicious activity monitoring
- Omnivore – MailChimp’s abuse-prevention initiative
- Legal counsel for compliance with privacy regulations

Perhaps one of the most impressive things MailChimp offers is a copy of its SOC II report. I filled out the form and honestly stated that I wanted to see a copy for research purposes, but, unfortunately, didn’t hear back.

4.4 Yahoo

Yahoo states that protecting its systems and users’ information is of paramount importance.

Some key points it mentions are

- TLS
- 2FA
- Secure storage
- 3rd party security
- Employee education
- Incident reporting process.

4.5 When Theory Meets Reality

Alongside these, most large companies such as Amazon, Twitter, Microsoft, Netflix, eBay, etc. all have impressive pages that explain how they take security seriously. A cursory search reveals many other lesser-known companies with similar claims.

However, the reality doesn’t always match the expectations that have been set. Nearly every one of the above-mentioned companies have suffered a breach of some description at one time or another.

Does this create an impasse of sorts? If large, well-funded companies that tick all the boxes when it comes to taking security seriously still get breached, is this ultimately an exercise in futility?

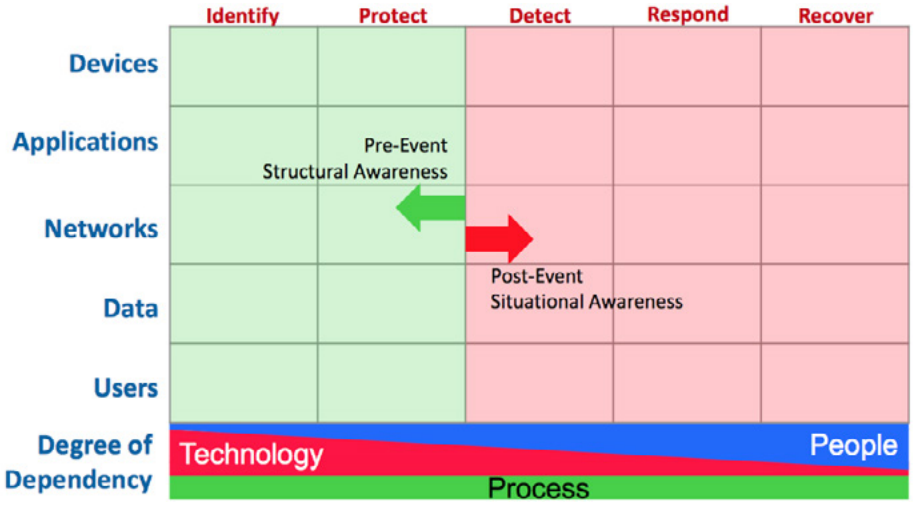
> *The only way I could really believe that statement is if there’s any proof of independent review of the way they do their operations (e.g. 3rd party audit to gain PCI DSS attestation, or similar). Of course, would help if the auditor is also a well-known entity!*
>
> *Otherwise it’s just a case of trusting their word, and I’m a distrusting kind of guy - Sacha Dawes*

5. When the Going Gets Tough, Security Gets Serious

> *This is going to sound weird, but a highly public breach is like a battle scar. It's all well and good to Talk the TalkTalk, but if you act like them, you're going to rightly get the pasting you deserve. Good breach handling requires communication with shareholders and the public, good timing and a commitment to do the right thing by customers even if it's going to cost you a bit more. The payoff from a well-handled breach is that people know you're under attack and can verify that you know how to handle yourself. Nobody wants to be known for having Equifax grade security, not even Equifax. - Steve Lord*

Perhaps one of the most spurious correlations when it comes to security is relating a breach, or lack thereof to the level of security seriousness. It's akin to me claiming that because I have been punched fewer times in my face than Mohammed Ali, I am a better fighter than he was.

Security is a lot more than merely preventing a breach, identifying assets or training staff. In fact, according to Sunil Yu's 2016 RSA presentation on understanding the security vendor landscape using the cyber defence matrix, he placed a greater emphasis on "post event" security that includes detection, response, and recovery than on prevention. Interestingly, the further along you go on the timeline, the more the reliance on technology decreases, while the reliance on people increases. This reflects the responses of the experts in this report who emphasized the importance of a solid security team rather than just the right tools.



> *It would be best if I knew some of the staff and had some insider knowledge on how they addressed security issues. - Wendy Nather*

5.1 It's Not A Matter Of If, But When

Many security marketing departments will tell their customers that a security incident is inevitable : that it's no longer a matter of if, but when.

Taking any marketing bias out of this - the reality is that being attacked or compromised by an external or internal party isn't a black swan event that falls outside of the norm. It's actually very much a part of everyday life.

It's how a company reacts during these times that will ultimately shape the wider opinion about how seriously it takes security.

Sadly, the only way that we get a glimpse of an organization's security seriousness is only after a cybersecurity event. Then, the organization's response is the best indicator of the veracity of the usual "we take security seriously" mantra. Questions such as, "was the data encrypted", and "how long did it take to notice the event" are usually answered as a result of these unfortunate events. - Bob Covello

5.2 A Matter of Intent

One could say that ultimately taking security seriously comes down to intent. While intent cannot be measured, during the course of the research, a few key themes emerged, which are worth highlighting.

5.2.1 No Tools? No Problem

Security seriousness doesn't need to be tied to specific tools or technologies. You don't necessarily need 'best in breed' technologies to be taking security seriously, or to do a good job securing your systems. In fact, having tools that are good enough for the purpose, coupled with the right people and processes can produce far greater results than best-of-breed technologies can ever do alone.

5.2.2 Blind Faith Security

There are many companies that invest in security blindly, giving the impression that on the surface they have done the right things: ticked boxes, made pledges and have proper security measures in place. But beneath the surface, there is often little understanding as to 'why' they're investing in security, hich is a situation that can sometimes end up being worse than not investing in security at all.

Passwords are a particularly good example of this. They were a funny thing even in my first role 18 or so years ago. Back then, we had a policy that dictated how passwords should be. The length, the strength, the expiry and rotation. Seriously, I had milk bottles that I kept longer than my passwords back then.

Users would have to reset the password every 90 days - and a lot of systems and companies still enforce that rule today, presumably in a bid to foil the 91-day clockwork cyber-pirates. The problem is they're like the 5 monkeys in a cage with one banana. Any time a monkey goes for the banana all of them get hosed down with cold water. All the monkeys soon realized that it was a bad idea to go for the banana. When one monkey was removed and a new 'dry' monkey was introduced - if it went for the banana, all the other monkeys would beat it up because they didn't want to get hosed down. One by one the monkeys were removed and replaced until you had all new monkeys in the cage that had never been subjected to a hosing. Yet, when a new monkey went for the banana they'd all beat him up; because that's the way things have always been done.

When I look at how a lot of companies are doing security - they look like those monkeys in the cage. You ask them why they follow something and they say it's because of policy - or because that's how it's always been done.

When you ask many of the companies that still force their employees to reset their passwords every 90 days, "why is that?" they'll say "it's our policy" - but they usually can't offer more of an explanation as to why. Some of them will try to quote something like a standard. I used to quote the orange book - the DoD's Trusted Computer System Evaluation Criteria (TCSEC)

Blindly following an ancient book without regard to the facts or the applicability of it is … I can't think of a the right metaphor – but it'll come to me.

5.2.3 Learning From Mistakes

Many security professionals will often quote Mike Tyson: "everyone has a plan until they get punched in the face."

However, when it comes to how seriously a person takes security, it's also important to observe how well they react to and learn from their mistakes. When a breach occurs, it is common for companies to send a communication to

affected users stating what happened and advising them to change their password, followed by an update on what the company has done to ensure that it won't happen again.

Any company that doesn't do at least this minimum immediately raises eyebrows as to their competence, and people question whether they are giving the matter the due attention it needs.

5.2.4 Continuous Conflict

Working in security can sometimes feel like working in a constant state of conflict. You're working against upper management, trying to secure budget; competing against other teams for resources; and fighting against the threats that are trying to take your systems down, extort ransom, steal your data, use your compute power, make a political statement, and so on.

But conflict isn't necessarily a dirty word, and it's not something that security teams that are serious should shy way from. Rather, conflict is something that should be embraced.

As Nasim Taleb states in his book "anti-fragile", the fragile breaks under stress, the resilient bounces back to its same state after stress, but the anti-fragile gets stronger with stress. Taleb likens anti-fragility to the Hydra from Greek mythology. Whenever its head was cut off, two would grow back in its place, so the Hydra became stronger with adversity. (although even the most anti-fragile systems will eventually collapse under too much stress).

5.2.5 Getting Your Hands Dirty

Security is not something that can be practiced in isolation. When an incident occurs, the world's spotlight shines brightly on a company's mistakes. However, a CISO or delegated security practitioner should not be afraid to jump in - even if that means mistakes will inevitably be made in the process.

In the wake of an incident, don't be afraid to write a blog, speak to the media, or be in the company booth at a trade show to speak to people directly and reaffirm to them how and why you take security seriously.

Being serious about security isn't something you can just say and move on. This is a relationship built on trust, and you need to continuously cultivate that trust. Like in any relationship, things won't be perfect and mistakes will be made, but if they are, buy a bunch of flowers, say you're sorry, and work in earnest to make things better.

> ***State of their security mindset: Is security part of what they do or is it obviously "say what customers want to hear"? Do they refuse to answer questions because "we don't talk about that because we don't want to give attackers our secrets"? Do they understand the current state of the threat environment? - Martin Fisher***

6. Are We Any Wiser?

> ***The "we take security seriously" line is the security equivalent of the infamous call center "your call is important to us" line. Everybody says it because that's what you say.***
>
> ***Taking security seriously is not a statement to be made, it's achieved by making security part of your process, and that's visible to everyone. - Scott Helme***

Taking security seriously isn't measured by a solitary point in time, nor can it be boiled down to implementing a single standard set of controls. There are many factors that contribute to this mindset.

If someone says they take security seriously, they should be able to defend that statement in some manner. It doesn't need to be a universally accepted position; it just needs to be something that shows they have put some thought into it and arrived at a logical conclusion.

Security doesn't always need to be visible. It doesn't need to be done for 'show' - a "security theatre" if you will.

The problem today is that too many companies don't think about security in earnest at all - well at least not until they get breached. After a breach, however, they all inevitably state: 'we take security seriously'.

The Japanese say you have three faces. The first face, you show to the world. The second face, you show to your close friends, and your family. The third face, you never show anyone. It is the truest reflection of who you are.

Similarly, you could say that security has three faces. The security you show to the world, the security that is visible internally in your organization, and the third reflects how you truly feel about security - that is the real measure of how seriously you take security.

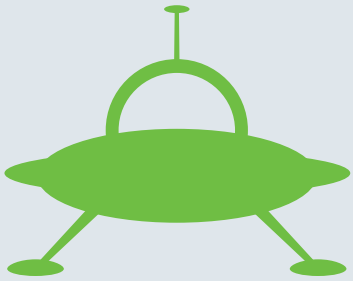
About the Author

Javvad Malik is the Security Advocate at AlienVault.

Previously, Javvad was a Senior Analyst at 451's Enterprise Security Practice (ESP), providing in-depth, timely perspective on the state of enterprise security and emerging trends in addition to competitive research, new product and go-to-market positioning, investment due diligence and M&A strategy to technology vendors, private equity firms, venture capitalists and end users.

Prior to joining 451 Research, he was an independent security consultant, with a career spanning 12+ years working for some of the largest companies across the financial and energy sectors.

As well as being an author and co-author on several books, Javvad was one of the co-founders of the Security B-Sides London conference.



About AlienVault

AlienVault®, an AT&T Company, has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our phenomenal and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management®, with the power of AlienVault's Open Threat Exchange®, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource constrained IT teams.