Cyber Resilience Crash Course

UpGuard™

About this Handbook

Who is this for?
This handbook is designed for business executives and other senior managers interested in looking at cyber risk from a business perspective and interested in building digital processes that are resilient to breaches and outages.

What will be covered?
We will take a look at how cyber risk is created, what data breaches mean to organizations in the real world, and what can be done to build a resilient digital business. Do you have company data in the cloud? We'll also cover how to prevent it from being exposed to the internet.

What is UpGuard?
UpGuard is the world's first cyber resilience platform. We help businesses understand, mitigate, and predict cyber risk. We'll include a few examples of how we do this later in the handbook.

Introduction

Technology and Information

How much digital technology is required for your business to operate? Unless this document has traveled back in time, the chances are quite a lot. Now consider how much digital technology your vendors require to operate. The scope of technology grows quickly when you consider how vast the interconnected ecosystem of digital business really is. But digital business isn't just about technology, it's about information. For many companies, the information they handle is just as critical as the systems that process it, if not more so.

Both technology and information bring great value to business. Technology enables wider reach, faster operations, global scale, and process automation. Information allows for analytics, which in turn enables companies to better understand their customers, their products, and their work— in short it enables understanding. But along with this value, technology and information also bring risk to business. Servers failing, the network going down, the website malfunctioning, the order database getting lost or corrupted— the list of the ways technology failures can interrupt business goes on and on. But even more dangerous are the risks associated with information. Data breaches can expose sensitive customer information, proprietary business information (trade secrets), information gathered and aggregated for analytics, or corporate operating information such as emails and internal documents. Each of these types of information brings great value to the company, but if exposed to the internet or taken by attackers, can bring the entire company down instead.

Business and Trust

This is because businesses run on trust. The relationship between a business and its customers is one grounded on the mutual trust that each party will fulfill their end of an agreed upon deal. For today's digital businesses, this is also trust that information provided by (or gathered on) individuals will be safeguarded by the business so it can't be used for any purposes other than those agreed to by the individual when he or she established a relationship with the business.

When this trust is broken, the image of the business as a single entity, the brand, is tarnished, sometimes irreparably, in the eyes of the customers. The business has failed to uphold its end of the deal, allowing the information granted to them in confidence to be accidentally exposed to untrusted third parties. To avoid this fate, businesses who rely on technology and information must start accounting for the risks they present. We call this cyber resilience.

What's Happened So Far

But what does all of this mean in the real world? If you've been following the news in the last decade, you probably already know. The disparity in scale between the simple misconfigurations that can leave information exposed and the potential consequences of those misconfigurations can't be overstated. Let's examine a recent example where a minor operational oversight led to global consequences and see how cyber risk is created and how it affects organizations.

RNC Contractor Data Root Analytics Exposes 198 Million Voter Records

UpGuard's cyber risk research team uncovered an exposed dataset containing the personal information and voting behavior of nearly every registered American. This wasn't data that was hacked, or socially engineered, or that required any type of technical proficiency and know-how to acquire. It was accessible to the public internet, the same as google.com.

How does this happen?

Data Root Analytics (DRA) was storing this data on the Amazon cloud, in a storage instance known as a Simple Storage Service (S3) "bucket." These buckets are used all the time by companies handling extremely large datasets during the process of their analytics or warehousing, often ephemerally, meaning they will open a bucket, store data there for some period of time, and then destroy the bucket. They are secured by a set of permissions, some of which allow anonymous public access. During whatever process DRA used to open the S3 bucket and upload the voter data to it, the anonymous public access permission was overlooked.

Here's the thing, though. The data didn't really "belong" to DRA. It was for use by the RNC. When the RNC outsourced their analytics processing to DRA, they took on the risk of DRA's information practices. The consequences of the exposure will have ramifications for both organizations, because although DRA was responsible for the exposed data, it was with the RNC that individuals likely feel they had developed a trust relationship. Because of the size of the data set— 198 million individuals— the consequences of that breach of trust will be far-reaching.

The Future

Because of the immense value delivered by cloud storage and hosting, this problem is likely to continue well into the future. Furthermore, as data techniques and analytics become more sophisticated, data sets will grow yet larger, increasing the risk posed by a single breach. For companies to grow and succeed they must take advantage of technology and information, but they also must place an equal amount of effort into mitigating their attendant risks. To not do so undermines the very business that technology and information are meant to improve.

Process Determines Product

How can such risks be mitigated? Not through what has traditionally been called cybersecurity. Companies have spent billions on cybersecurity in the last few years, only to see breaches proliferate. This is because cybersecurity assumes that you are protecting yourself against an attacker. It is perimeter focused, external, searching for activity and communications that in themselves are suspect. None of this begins to touch the true problem, which is this: the complexity and scale of digital operations results in misconfigurations that leave systems and data vulnerable.

More likely: a hacker breaking through your firewall, taking over a server, and accessing data, or a systems administrator setting up a temporary storage instance, moving data to it, and forgetting to check one of the many boxes that ensure a hardened configuration? It's the processes by which IT operations are carried out that ultimately determine whether production systems and data are resilient. Trying to drape security on top of an existing IT ecosystem is futile. It needs to be built in, at the process layer, through testing, validation, and automation.

Take the cloud. Leave the breach.
What companies want is to deploy storage quickly, at scale and over time, without running the risk of public exposure. Manually setting up one S3 instance might seem simple, but a team of people setting up and tearing down dozens every day presents several major challenges. First we need to state our policy.

Cloud storage used to host company data must be tested for compliance to security guidelines as part of the provisioning process, and at regular intervals throughout its lifetime to ensure company data is kept secure.

Easier said than done, though, right? That all depends. An automated provisioning process can incorporate compliance validation directly, meaning that all new S3 instances would be tested for anonymous public access. Those which were publicly open would fail the validation, which could then trigger a remediation action, or at the very least, notify an administrator or create an incident ticket.

UpGuard tackles this problem with Procedures, which outline and automate common steps for asset provisioning, hardening, migration, and other common IT operations. We can add scanning S3 buckets to our procedure, along with tests that verify the other aspects of a cloud deployment. These procedures can run as part of a larger automated process, and by themselves as regular maintenance checks. By automatically verifying the configuration state details and proactively addressing misconfigurations, we can ensure that company data will not be publicly exposed in the cloud.

The complexity and scale of digital operations results in misconfigurations that leave systems and data vulnerable.

Cyber Risk is a Business Problem

The days of relegating IT issues to the tech gurus in the basement have come and gone. Information technology is so integral to business today that it must be taken as a serious facet of the company, one that must be strategically integrated and understandable to business leaders. When a big breach hits, media, customers, and shareholders will look to the C-Suite for answers, not the person who set up the cloud server. This means the C-Suite should be well-informed about the risks posed by their technology, and have an opportunity to mitigate those risks through internal measures and cyber insurance.

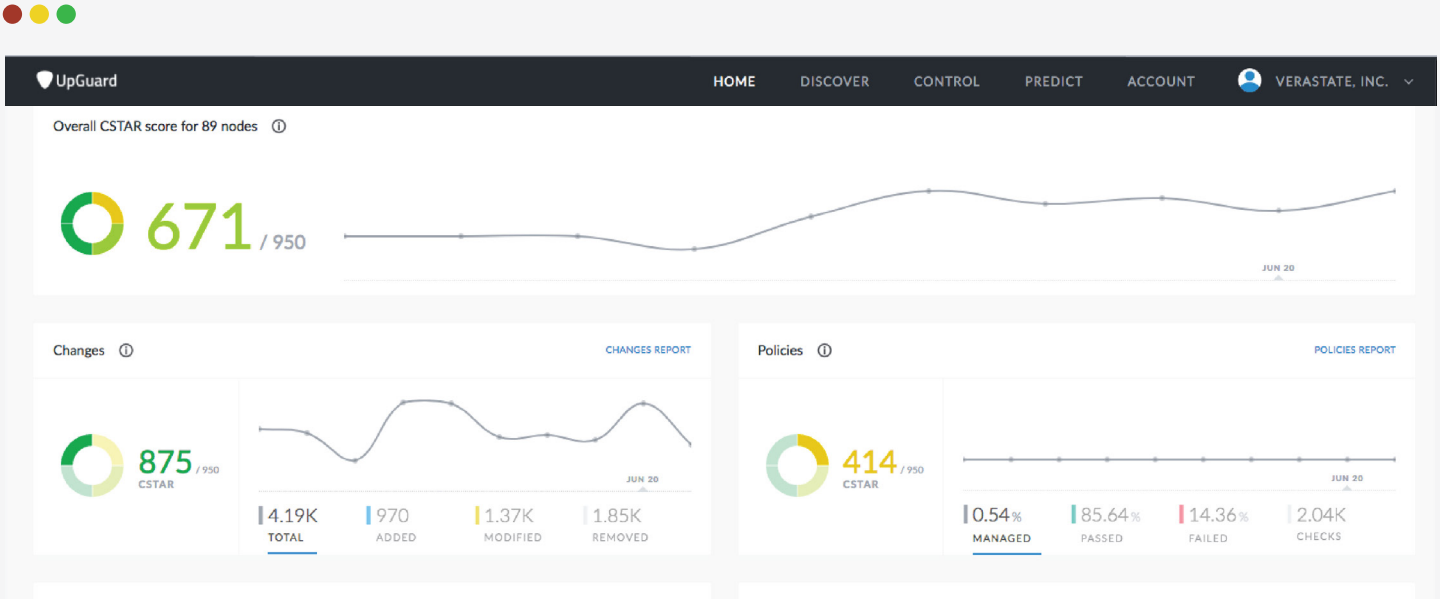
Out of Sight, Out of Mind

The abstract nature of information, and the intangibility of the technological ecosystem make understanding cyber risk extremely difficult, even for the most technical people.
Cyber risk needs to be visualized and made tangible to be considered alongside other business concerns. This picture of cyber risk must be comprehensive to be effective.

This includes both external, perimeter-based information, and internal asset and process information— the entire digital footprint. A partial picture creates risk blindspots. It doesn't matter from what angle information is exposed, just that it is, which means all facets must be covered for optimum resilience. This includes vendor risk, for as we saw above, it is often a third party through whom data is breached.

Process Determines Product Revisited

The internal portion of this risk assessment should include not just assets and information, but processes themselves, information about the cadence at which things happen and how successful they are. For instance, how often servers are patched, or how often configurations are validated, or how well assets comply to company policy are all risk vectors that ultimately determine the likelihood of a breach. Collected over time, these assessments can reveal trends of improvement or decline and help prioritize spending and labor in the effort to mitigate cyber risk.



CSTAR With UpGuard

UpGuard gathers information from four key risk sectors: changes, vulnerabilities, policies, and external. These four sectors are then aggregated into a single score that represents the total enterprise cyber risk called CSTAR. This telescopic view, from biggest picture to technical detail, allows businesses to not only understand their cyber risk, but proactively reduce it.

Changes
A healthy environment changes all the time, but there's good change and bad change. UpGuard validates good changes, verifying that changes achieve the expected results. It also catches unauthorized changes, as well as changes that pose security risks, and automatically surfaces them for remediation.

Vulnerabilities
Nearly all successful attacks exploit known software vulnerabilities. Running vulnerable software in an enterprise environment drastically increases the risk of a breach, outage, or ransomware attack. UpGuard gathers vulnerability data from all assets and determines where vulnerable software is running, so assets can be hardened before an attacker finds a way in.

Policies
UpGuard's policies act as executable documentation, ensuring that IT assets conform to company standards, regulatory mandates, and third party hardening benchmarks. The more assets covered by policies, and the rate at which they conform to them, determines how the assets are scored. Testing the actual configuration against expectations is the only way to be sure assets are resilient in production.

External
The previous sections have focused on the internal data UpGuard can gather within an environment. The final section of the CSTAR assessment looks at the organization from the outside, assessing web, email, and DNS configurations for all associated domains. UpGuard also includes external profiles of third party vendors and services, ensuring visibility into the assumed risk of the entire supply chain.

Resilience, Insurance, Change
Ultimately cyber risk is a question of resilience, how well can your digital environment withstand the forces that would harm it. Measuring that resilience requires insight into the totality of the datacenter, as well as the processes that create and change components within it. That's a massive amount of data that needs to be distilled down to a handful of prioritized insights. But an accurate picture of cyber risk can also help close the risk gap by allowing for accurate scoping of cyber insurance. The cyber insurance model is in its infancy, but the more data that can be used to form an accurate risk model, the better policies can be scoped and updated for particular organizations.

Finally, cyber risk is dynamic. It's not something you check every year, or every quarter, or every month, but something that can fluctuate day to day: when someone accidentally leaves a port open, forgets to change a default password, doesn't lock out anonymous public access, or any of the numerous errors that can lead to a major breach. Cyber risk needs to be evaluated at its own speed, and in the modern enterprise, that's near real time.

There is no security by obscurity when the stakes are this high.

Conclusion

Information is valuable. That's why you use it in your business, and it's why you should protect it from accidental exposure. Because the value of data rises across the board. It becomes more dear to the individuals whom it's about and to those who would seek to exploit it. For example, you might be familiar with a cyber attack known as spearphishing, where a highly-targeted email is sent to someone trying to trick them into disclosing information or transferring funds. Imagine how successful these attackers could be if they obtained an analytic data set from exposed cloud storage. There is no security by obscurity when the stakes are this high.

Further, information is given and handled with the trust between a customer and a brand. When that information is misused, neglected, or otherwise exposed to third parties, that trust is broken. One need only examine the reaction to major data breaches on social media to see how upset and vulnerable it makes people feel when their information is laid bare. The gap between business operations and IT operations must be bridged, so that businesses can take advantage of the value information technology offers without being undone by the risks it entails.

UpGuard is the world's first cyber resilience platform, designed to proactively assess and manage the business risks posed by information technology.
By validating and automating IT processes, we help organizations build resilient digital businesses on-site and in the cloud.

909 San Rafael Ave.
Mountain View, CA 94043
+1 888 882 3223
www.UpGuard.com