Cyber Resilience for the C-Suite
What is cyber resilience?

The definition of cyber resilience is simple: the ability to assess, measure, and mitigate risks posed by technology to the organization deploying it. Understanding how cyber resilience works and why it matters isn't quite as simple, given the long and tangled history of digital business. Let's take a look at what cyber resilience is and the context from which it emerged.

Why do businesses use technology?

The benefits of technology seem self-evident, but examining exactly why businesses use technology will help us understand why a resilience strategy is necessary. Technology brings value to business in a number of ways:

- Speed - Do it faster.
- Efficiency - Do it better.
- Scale - Do it bigger.
- Functionality - Do it more easily.
- Effectiveness - Do more of it.

No matter what industry you're in, success depends upon the ability to keep growing, and technology provides the means to do so. Imagine trying to compete in today's marketplace without using computers or the internet. But despite the obvious advantages, technology also brings risks to business:

- Unreliability - Can't do it at all.
- Insecurity - Can't do it safely.
- Untrustworthiness - Can't do it privately.
- Complexity - Can't do it without specialized knowledge.
- Obsolescence - Can't do it the same way forever.

No matter how much value technology brings to business, if the risks it poses are too great, such value becomes moot. Cyber resilience is the practice of minimizing the risks technology poses so that technology's value can be fully realized.

Cyber risk is business risk

As technology is deeply integrated into modern business practices, technological risk and business risk are indistinguishable. If you can't do business without your technology - and most enterprises can't - the risks of that technology are the risks of your business. Business risk isn't new, and like this older form, cyber risk should be addressed at the top levels of the business to ensure the organization's health and survival. However, that can be easier said than done when IT is siloed from management, and strategic knowledge can't be communicated effectively. It is crucial that businesses have high-level visibility into their IT operations to better assess, measure, and mitigate potential risks, for as we'll see, it is business leaders who are ultimately held accountable in the event of a breach or major outage.

Cybersecurity is dead

The data center's opacity to business leaders has led to twenty years of ineffectual cybersecurity spending, with billions put toward silver bullet solutions meant to stack on top of whatever environment you have, supposedly protecting you from attacks. But despite hemorrhaging money for cybersecurity, breaches
and other attacks have increased in number, sophistication, and success rate. Why?

The answer is simple: the majority of breaches and unplanned outages occur due to misconfigurations. It doesn’t take a hacker to walk through an open door, and when a server or database is left exposed to the internet, or lacks a hardened configuration, that’s exactly what it is for anyone who wants it. A six-figure network protection device isn’t going to stop assets from being deployed incorrectly. It isn’t going to stop unplanned change from creating problems down the road. It isn’t going to fix the server patching process. These are the areas where the most business risk is created-- not flashy zero-day exploits or other vague hacker magic. The sheer complexity of a modern data center is enough to ensure exploitable misconfigurations. The key to cyber resilience is having a scalable, repeatable process for finding and fixing them as quickly as possible, before someone else takes advantage.

Day-to-day operations
Every day new systems are deployed, configuration changes are made, updates are released and installed, and new applications are rolled out. The day-to-day work of IT does more than just keep the lights on-- it determines how resilient the business is to technological risk. If the process for deploying a new server includes steps to harden and test it, the business is less likely to have vulnerable servers in production. Likewise for every IT process. Cyber resilience is about becoming aware of the impact these processes have on the big picture and improving them to create a more resilient whole. While newer businesses might be able to implement better technological processes out of the gate, businesses whose technology has grown organically over time may be faced with a tangle of issues and de facto processes that need to be repaired to achieve resilience. Understanding how to build resilient assets and processes is key to make this transformation possible.

Testing, measuring, feedback loops
Data-driven methodologies should govern how processes are changed and determine what success looks like. Only testing of the actual state of your environment can validate whether or not it’s good, and what needs to be changed to make it better. Good processes produce usable metrics, giving the people involved a clear and concrete way to understand what they are doing. Over time, these measurements should reveal trends and patterns to which the company can react, ensuring that stale processes don’t become weaknesses. Furthermore, it is these metrics which provide visibility for business leaders into the posture of the technology upon which they rely. This is the final layer of a cyber resilience strategy-- using data to make decisions with agility and confidence.

Why should businesses move to a cyber resilience model?
Cyber resilience is a paradigm shift for how enterprise IT is done. But change isn’t always easy, so why should businesses adopt this method?
Business requires trust
From the smallest company to the largest corporation, business depends on trust. If a customer can’t trust a business to deliver, or a business can’t trust a customer to pay, that trust deteriorates rapidly. Although business relationships have been largely abstracted with technology, that fundamental idea of trust remains solid. When a customer trusts a business, they actually become part of a series of interdependent trust relationships. IT teams trust their technology to work. Business leaders trust their IT teams. Customers trust the business.

If an unexpected outage makes service unavailable, or a breach reveals sensitive information, the customer’s trust in the business is damaged. They’re not mad at the firewall, or the network administrator, or the IT manager, but at the business itself. Protecting the customer relationship now means ensuring that technological risks don’t disrupt a brand’s reputation.

Digital Backlash
The consequences of this disruption will ultimately lead to a digital backlash, as companies that do not prove resilient begin to fail in the market against to those that do. Cyber incidents such as a data breach or major outage continue to take larger and larger tolls on companies, who have seen everything from sharp stock price drops to legal action by affected customers. Reputational damage is amplified by short news cycles and social media, while the expectation by customers for technological competency and data handling has never been higher. Failure to account for cyber risk now will prove disastrous in the future.
Who takes the fall?
We don’t need to look into the future to see the damage done, however. Plenty of prominent breaches have already occurred, and many big name executives have taken the brunt of the blame. As mentioned above, the customer forms a relationship with the brand, not with any particular piece of the business. When that relationship is violated, the customer wants justice from the brand, and only a CEO or other high-ranking executive represents the brand enough in their person to act as a sufficient receptacle for blame. It doesn’t matter if a contractor forgot to close a network port, or a sysadmin left a default password on a database-- however the breach occurs, the response must be equal to the consequence, which for millions of rows of customer data can mean an executive’s job, and perhaps even their career. This is why business leaders should have high-level visibility into IT operations, and a stake in the risks posed to the business by the technology on which it depends.

Third party risk
No business is an island. Data is now shipped through multiple suppliers and vendors, sometimes crossing the world and back to be processed and stored. However, outsourcing data tasks to a third party also means outsourcing the risks as well, but not in a way that protects the company. We’ve seen that even if a third party vendor is ultimately responsible for a data breach or outage, the primary company is held accountable. Just as a customer doesn’t care about the technical details of how a breach occurred, they also don’t care about the inner workings of the business. Whether data was shipped to a third party vendor or handled in-house, the relationship between the customer and the primary brand suffers when a breach occurs.

Assessing vendor risk is therefore necessary to determine which third parties can be trusted to handle data and perform other technological duties. Since cyber resilience is a holistic practice, all links in the software and data chain must be factored in to create an accurate picture.

Visibility creates opportunity
Finally, resilience isn’t just about staying afloat amid unending threats, but having the agility and understanding to act on opportunities. Innovation is about taking risks, and the better you understand your current environment and how it operates, the more informed you will be about those risks and whether or not they are worth the possible benefits. Automated processes and validation coupled with thoughtful metrics and short feedback loops make experimentation possible and fruitful, without disrupting business function. Cyber resilience isn’t just about making technology better for business, but making business better using technology.
Who cares about cyber risk?

**Customers**

If you asked random people “do you care about cyber risk,” they might not say yes right away, but people do care about their information being protected. They do care about whether the services they need are available when they need them. Ultimately this is what cyber risk boils down to for the average person: can I trust the companies I use? Before considering cyber risk from a business perspective, consider it from your perspective as a consumer of other products and services. What do you expect from your bank, your health insurance provider, your favorite online store? How can you provide the experience you want for your customers? Build something people can trust.

**CEO**

Cyber resilience starts and stops at the highest level of the business. It comes down to a choice: will the business account for the risks inherent in the technology it uses and integrate IT infrastructure and processes into the business strategy? Or will it see IT merely as a cost center, ancillary to the main business— a relatively low priority? Buy-in has to start at the top and filter down for a cyber resilience implementation to succeed.

**Concerns:** Business risk

**Key Metrics:** Enterprise risk score

**How UpGuard can help:** Top level visibility means summarizing a massive quantity of operational data as simply and accurately as possible. UpGuard’s cyber resilience platform includes CSTAR, our cyber risk score, which quantifies technical details and translates them into business risk visualizations.
CFO
IT budgeting can be a frustrating process. For many CFOs, cybersecurity spending has been spiraling out of control, without evidence of marked improvement. IT managers regularly hit obstacles trying to obtain funding because upper management doesn’t prioritize their concerns. This antagonistic relationship increases business risk, as strategic goals break down between departments and low morale leads to circular processes and obscure goals. To make the business resilient, CFOs must work with IT management to ensure that spending is directed appropriately. For IT managers, that means providing the CFO with accurate metrics over time that support purchasing decisions. For CFOs, it means reprioritizing IT spending to improve processes; working with the CEO to mitigate business risk, including scoping and pricing cyber insurance policies; and assessing third party vendors.

Concerns: Budget, insurance
Key Metrics: Yearly/quarterly reduction of risk, vendor risk assessment
How UpGuard can help: UpGuard tracks your risk over time with CSTAR, highlighting trends, patterns, and progress of cyber risk mitigation. Because CSTAR represents the totality of an organization’s risk posture, UpGuard includes vendor and third party risk assessment as part of that calculation. Vendors, partners, and other external entities can be added as nodes within the platform so the cyber risk assumed through business relationships is never hidden.

CIO/CTO
Top-level IT management should be ultimately responsible for process improvement and measurement. Working with middle management, CIOs and CTOs should ensure documented, tested processes are used for common tasks. Processes should yield important metrics that help shape strategic direction. As important as agility is in technology, processes can rust and become counterproductive. CIOs and CTOs should ensure that processes help people do their jobs, not act as administrative bottlenecks, piling on top of an already full workload. This is why automation strategies are so important to successful IT processes.

Concerns: IT process performance, strategic direction
Key Metrics: Process improvement over time (For example, number of incidents raised on new servers, patch deployment cadence), detailed risk scoring
How UpGuard can help: UpGuard’s cyber resilience platform integrates with incident tracking systems so that the process work of change management can tie directly into the actual state of the environment. This allows planned changes to be validated and unplanned changes to be automatically caught and raised as incidents. The CSTAR risk score is subdivided into four areas: changes, policies, vulnerabilities, and external risk. This allows upper IT management to drill into the risk score and understand exactly which assets and procedures need to be shored up.
CISO

CISOs should ensure that assets and data conform to company policy. This means both establishing and maintaining that policy over time as things change. A company policy might include in-house build standards, regulatory compliance mandates, and third party or industry benchmark standards such as NIST or CIS. Regular vulnerability testing should be performed under the CISO's guidance to ensure utilized software is secure. The CISO should have total visibility into the state of the environment and how well it complies with company expectations.

Concerns: Asset and data security and privacy
Key Metrics: What percentage of assets are validated against policy? What percentage pass?
How UpGuard can help: Validating assets against policies is the only way to know whether or not those assets can be trusted. Is there an accidental open port? A default or missing password? An insecure configuration? UpGuard proactively answers these questions so problems can be remediated before they are exploited by outside actors. It also retains and displays metrics based on policy coverage and success rate, so CISOs can fully understand which pieces of their environment should be trusted.
How does a business become resilient?

Now that we've looked at what cyber resilience is and why it's important, let's take a look at how to make it happen. We've talked a lot about processes, testing, validation, and automation, but let's see how this all comes together in the real world.

**Know what you have**
The first step toward resilience is getting a comprehensive picture of your digital environment. This means internal and external assessment, as well as of third-party vendors. Every server, database, network device, application, and website should be included, on-premises and in the cloud. Any omissions from this picture become blind spots for risk, potentially undermining whatever work you do to protect that which you know about. An environmental baseline should be established, including all of the configuration details of every asset. This baseline should be tracked over time to detect anomalies and discover trends.

**Know if it's good**
Once your baseline is established, you need to test it against your expectations. This can include company conventions, security standards, and other benchmarks. Without testing, there's no way to trust your environment. Testing provides the necessary validation to move forward with confidence. It's also the only way to provide useful metrics about IT processes and performance, metrics the C-suite needs to see into technical operations. Comprehensive testing can help identify areas for improvement and makes spending prioritization easier to determine based on risk.

**Know how to change it**
Once you know what you have and whether or not it's good, you can begin predicting next steps. Insights raised from this data can be used to course correct and reduce business risk. When properly visualized and contextualized, cyber risk can be understood and mitigated at the highest level. Furthermore, it can be quantified and tracked over time to understand improvement and catch declines before they become major problems.

**Conclusion**
Cyber resilience is the way technology needs to be used in the enterprise for businesses to succeed. It means proactively accounting for technological risks by building processes that mitigate them. Ultimately this reduces the likelihood of a breach or major outage by creating resilient systems that behave predictably over time. This protects businesses and customers, delivering secure and reliable services.
Businesses depend on trust, but breaches and outages erode that trust. UpGuard is the world’s first cyber resilience platform, designed to proactively assess and manage the business risks posed by technology.

UpGuard gathers complete information across every digital surface, stores it in a single, searchable repository, and provides continuous validation and insightful visualizations so companies can make informed decisions.

© 2017 UpGuard, Inc. All rights reserved. UpGuard and the UpGuard logo are registered trademarks of UpGuard, Inc. All other products or services mentioned herein are trademarks of their respective companies. Information subject to change without notice.