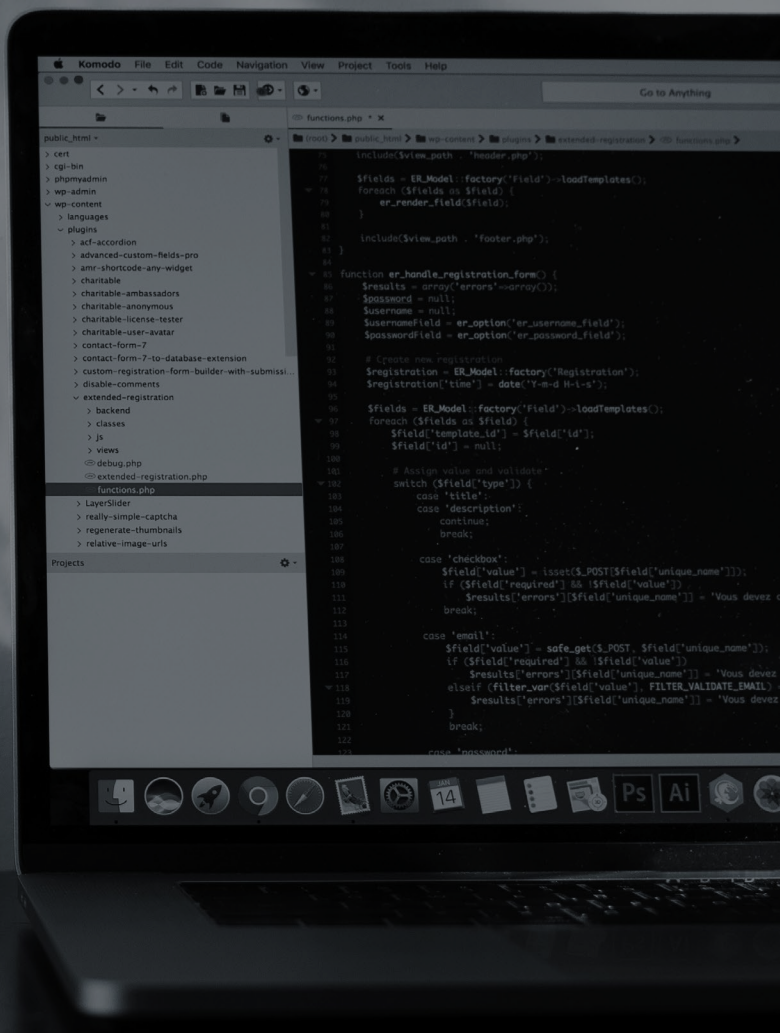
The Nontechnical Guide to Cyber Risk



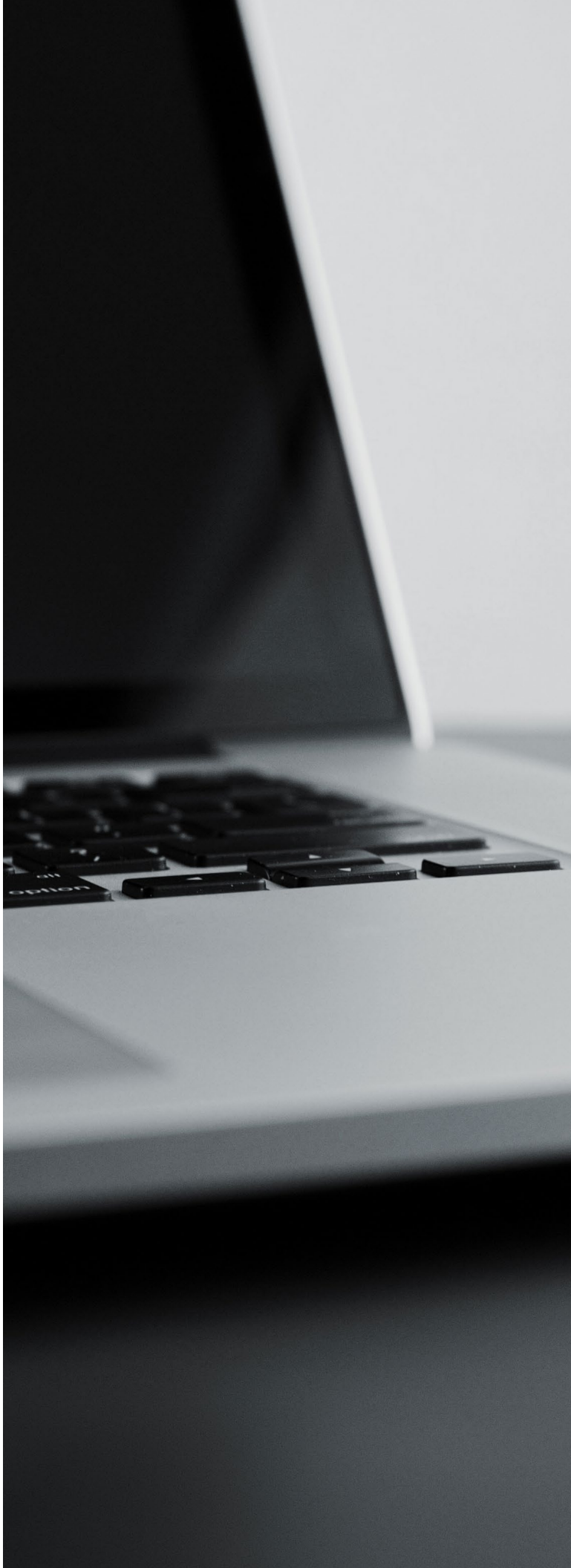
UpGuard

Introduction

This is the price tag of technological innovation: 300 data breaches every minute and almost 1 million new malware threats released every day, according to recent statistics. If this isn't sounding o alarm bells, you've likely been desensitized by the frequency of data breaches splashed across the news headlines. However, for most of us—including security professionals and vigilant consumers alike--the distressing surge in attacks is a sign that cyber crime is spiraling out of control.

In response to failing security measures, organizations are turning to new risk models for managing cyber threats to the business. Mass digitization has brought enterprises into uncharted waters when it comes to securing business assets against unknown threats; as such, methodologies for managing cyber risk are still nascent. Concepts like cyber resilience are taking root, however, and its strategies are resonating with forward-thinking enterprises—as are instruments for measuring and mitigating cyber risk like reputation scoring and cyber insurance, respectively.

The purpose of this guide is to equip nontechnical readers with the foundational knowledge and language for understanding and managing cyber risk. Though terms will be introduced, no specialized knowledge in systems and network administration or IT security is presumed. Upon completion, readers should have enough requisite knowledge to carry an intelligent conversation regarding cyber security and risk.



The Language of Cyber Risk

You don't need to be an IT security expert to grasp the fundamentals of cyber risk. That said, getting a lay of the cyber threat landscape is necessary to gauge your organization's cyber risk exposure. This involves familiarizing yourself with the language of cyber risk, as well as common threats and cyber attack methods.

Below are key concepts and terms used most frequently in conversations regarding cyber risk management.

Automation	The process of making routine and/or complex IT tasks self-acting or self-regulating. Manual processes often result in configuration errors and inconsistencies that in turn lead to security compromises. For this reason, automation is critical to security.
Continuous Security	A new approach that combines different layers of security for more comprehensive coverage. Continuous security allows firms to determine their security postures in real-time for effectively managing cyber risk on an ongoing basis.
Configuration Management (CM)	The tracking and management of detailed information describing a firm's computer systems and networks. Since misconfigurations are a major cause of data breaches, CM is critical to bolstering security.
Cyber Risk	The likelihood that a firm will suffer damages resulting from digitization (e.g., data breach, intrusion, or IT systems outage).
Cyber Threat	The method used by an attacker to gain unauthorized access to a system or network--usually to steal data like credit card information, distribute malware to other computers, or hijack proprietary information.
Cyber Resilience	Also referred to as digital resilience, cyber resilience is a combination of tactics for ensuring that cyber attacks don't impede or halt the business. A central tenet of cyber resilience involves taking calculated risks when the return on investment is high. And because data breaches are inevitable, the proper security mechanisms must be in place to protect the resources that matter the most.
DevOps	The merging of development and operations to build software and services better, faster. As of late, some of the values it espouses—collaboration, information unsiloing, automation over manual processes—are being applied to security, commonly referred to as SecDevOps/DevSecOps/Rugged Ops.

Exploit	A cyber attack that takes advantage of a specific vulnerability or flaw in a system.
Insider Threat	A malevolent actor originating from within a trusting organization (e.g., disgruntled employee).
Intrusion	The consistency of systems in an environment and the extent to which they remain in line with expectations
Yes	The unauthorized access of privileged networks or systems by a malevolent actor.
Patch Management	The processes a firm puts in place to regularly update software systems against security flaws. Because unpatched systems are a leading cause of data breaches, patch management is crucial to maintaining strong security.
Zero-Day (0-day)	A threat or vulnerability in a product or solution yet unknown to the vendor, developer, or manufacturer.

Common Cyber Threats

Despite the constant barrage of exotic-sounding exploits, the reality is that most data breaches and intrusions are neither imaginative or sophisticated. Furthermore, the 80/20 rule or Pareto's Principle applies to cyber threats as well—that is, approximately 80% of effects come from 20% of the causes. In the context of cyber security, this means that a handful of threats are used in the majority of data breaches and intrusions. Firms should therefore prioritize their security efforts to combat threats they're most likely to encounter.

The following is a list of the most common cyber threats encountered in the wild. Taking the appropriate measures to protect your organization against these items will drastically reduce the chances of a data breach or security incident.

Malware

A catch-all term referring to any type of software code written for malicious purposes (e.g., stealing or destroying data, launching cyber attacks). Malware commonly makes its way into a system or environment through email attachments, software downloads, and unremediated vulnerabilities.

Recently, the rise of cross-platform malware makes it easy for bad actors to launch attacks across different operating systems.

Metamorphic/polymorphic malware is considered by many to be the single biggest security threat to organizations. As its name implies, this type of malware is capable of changing its software code continuously, making it hard to detect and track with conventional security solutions.

Viruses, worms, Trojans, and bots are all classes of malware.

Phishing

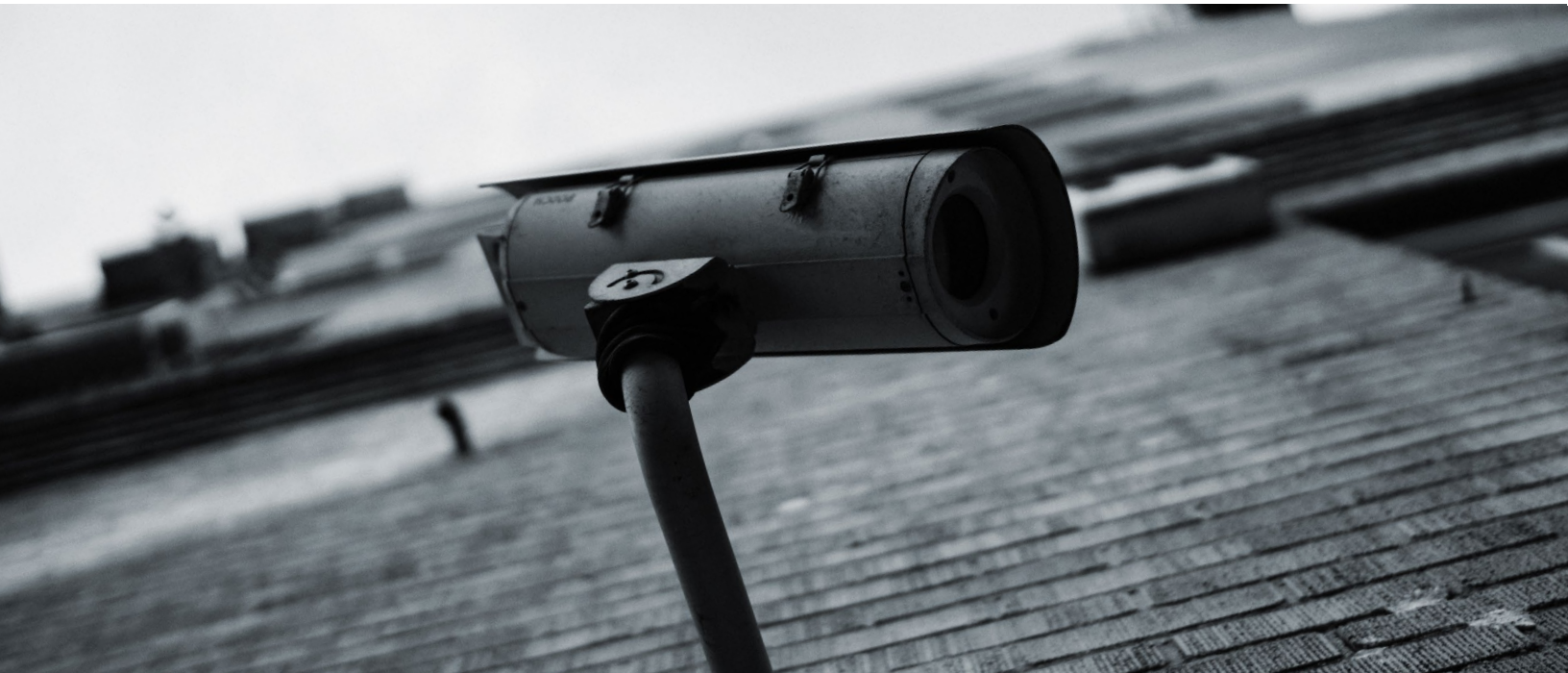
A type of threat that uses email to trick users into taking some form of action (e.g., clicking on a link, verifying account information, resetting a password).

Phishing emails commonly pose as legitimate financial institutions or popular online services performing regular or emergency maintenance. Users are then tricked into clicking on a link and entering their personal data.

Password Attack

A threat that involves a bad actor attempting to crack an existing authorized user's password to gain privileged access.

Denial-of-Service (DoS)	A cyber threat whose primary objective is to disrupt a firm's network or web services. For example, attackers may attempt to bring a popular website down by overloading it with connection requests. Distributed denial-of-service (DDoS) attacks use multiple computers to launch coordinated attacks against a target. DoS/DDoS attacks are carried out primarily to damage an firm or brand's reputation, as opposed to stealing its data or intellectual property.
Man in the Middle (MITM)	An attack that intercepts and relays privileged data shared between two parties by inserting the bad actor as a proxy. For example, a bad actor using an MITM attack to steal a online banking user's data would insert itself between the bank and user.
Drive-By Download	A compromise that results in a malicious program being downloaded and installed on a user's computer--just by visiting a website, no user interaction required.
Malvertising	A threat that involves cyber attackers uploading infected display ads to various ad networks. When the ad is clicked by viewers, malicious code is downloaded to their systems.
Rogue Software	These threats masquerade as legitimate software utilities: virus scanners, registry cleaners, and more. Viewers are prompted to download and install the software, but must first click a button or link agreeing to its terms of service. Doing so in actuality downloads the rogue software to the viewer's computer.
Advanced Persistent Threat (APT)	This type of threat consists of highly coordinated and sophisticated attack efforts using a multitude of intrusion methods. The APT is a favorite amongst cyber attackers engaged in high-stakes corporate espionage and intellectual property theft.



New Risk Models for Digitized Firms

Enterprise risk management hinges on a firm's ability to comprehend, control, and describe risks taken for achieving business strategies and outcomes. In the majority of scenarios, financial instruments—property, professional liability (E&O), and product liability insurance, among others--are available to offset the devastating impact of catastrophic events. When it comes to cyber risk, however, modeling for catastrophic cyber losses in the commercial insurance industry is still in its infancy. A myriad of challenges are hindering the development of accurate, standardized models for cyber risk assessment, including lack of actuarial data and the tendency for IT infrastructures to differ greatly--even between similarly sized/performing businesses.

Of course, this is less than ideal for creating a competent, overarching enterprise risk management strategy. There is no greater confidence buster for stakeholders than lack of risk awareness exhibited by the organization's leadership. What's missing is a cyber risk assessment framework that takes into account all the aspects of an enterprise that make it susceptible to being compromised. This includes such considerations as what type of security controls are in place, whether a patch management program exists, and how consistent are the systems' configurations over time, among others. These elements and more collectively make up a firm's security posture and cyber risk profile.

Introducing UpGuard's CSTAR

CSTAR is fast becoming an industry standard for underwriters and insurers to accurately benchmark and calculate an organization's cyber risk profile. The framework includes tests that measure both internal and external dimensions of a firm's posture, providing concrete answers to previously unanswerable questions like:
Compliance: How capable is the firm in maintaining its systems in a resilient state? Do these systems meet regulatory requirements?
Integrity: How capable is the firm's ability to validate change? How much unauthorized change is occurring in the environment?
Security: How capable is the firm's ability to detect and remediate vulnerabilities? Do any known vulnerabilities currently exist in the environment?
External risk dimensions exposed by UpGuard's free reputation scanner include:

Business: how is the firm's track record in terms of documented breaches and employee/public perception?
Communications: how strong are the firm's security controls for validating email authenticity and preventing fraudulent messages?

Website: do any critical website perimeter security risks currently exist?

By measuring factors both internal and external to the organization in question, UpGuard is able to accurately assess and package a firm's cyber risk profile in a single number—it's CSTAR score. This can in turn be used by underwriters and insurers for cyber risk determination and crafting insurance policies.

Conclusion

If there's one term to remember from the language of cyber risk, it's cyber resilience: protecting your most important assets while taking calculated business risks to remain viable-- rolling with the punches, so to speak. Acquiring the proper cyber risk coverage to ensure that catastrophic security failures don't capsize the business is part of the digital resilience equation; to provide this coverage, however, insurers and underwriters need a comprehensive framework for accurately assessing cyber risk that transcends traditional risk models. UpGuard's platform and CSTAR scoring system fulfill this need through a comprehensive, easy-to-understand solution for maintaining cyber resilience in today's digital landscapes.

References

http://www.warwickresource.com/blog/entryid/9501/there-are-over-300-securitydata-breaches-every-single-minute

http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

http://www.infoworld.com/article/2616316/security/the-5-cyber-attacks-you-re-most-likely-to-face.html

http://www.darkreading.com/perimeter/applying-the-80-20-rule-to-cyber-security-practices/a/d-id/1321818

http://www.techrepublic.com/blog/it-security/continuous-security-monitoring-wave-of-the-future

http://www.riskandinsurance.com/cyber-risk-models-remain-elusive/

http://www.theactuary.com/features/2014/12/cyber-catastrophe/

http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover

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.

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