NETSCOUT®

| WHITE PAPER |

The Continuum of Cyber Risk Analysis

SECURITY

The Continuum of Cyber Risk Analysis

As cyber threats evolve, so too must your cyber threat protection – thus the Continuum of Cyber Risk Analysis. Executives responsible for cyber security face increasingly difficult choices about what systems to invest in and where to allocate resources to best protect the enterprise. Typically, this falls to the IT executive, who is also challenged to communicate, and worst case, defend these decisions to their peers, the board, or regulators. Risk assessment is a critical tool in making these choices. With digital transformation, involving the collection and wider use of valuable data across broader, inter-connected networks, these challenges will only increase.

The assessment of business risk itself exists along a continuum, from rules-based, compliance models to qualitative, experiential based judgement assessments, to mathematically quantifiable calculations. As the successful enterprise has become reliant on extensive, inter-connected networks – and the target of sophisticated cyber criminals – IT in particular, requires the capability to better assess, quantify and communicate their decisions regarding cyber risk.

"As senior business leaders are becoming more engaged on the topic of cybersecurity, the need for a more practical and informed cybersecurity risk management capability is mounting"

Husam Brohi, Director, Cybersecurity and privacy, PwC

Rules-based Risk Management

Every industry is faced with more privacy and information security regulations: GDPR, FISMA, PCI-DSS, HIPAA, even state level regulations like the NY State Department of Financial Services 23 NYCRR 500, or California's new Consumer Privacy Act of 2018. Complying with relevant regulations must be part of any defensible security policy. Yet the notion that being in compliance means one is on top of risk, or that one is safe from network or information compromise, is a dangerous misconception. Regulations do not and were never designed to provide a real measure of risk. Virtually all data breaches have occurred to compliant organizations.

System control frameworks are also valuable components of a strong security posture. Some of the more common frameworks include:

- National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity, NIST 800 53 Rev 4 (soon to be Rev 5);
- Standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27001/27002;
- Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense, promoted by SANS Institute.

But controls too do not provide an actionable, communicable measure of risk – nor quantify the potential degree of damage to the business resulting from a cyber event.

The uncomfortable truth: compliance, rules-based risk management does not provide insight into the likelihood of a cyber compromise nor quantifiable impact of a breach. Adhering to regulations and installing more controls does not inform executives what is the probability of an event, nor if there is an event, how much it will actually cost the business. Perhaps even more damaging, passing audits and being in compliance can engender a false sense of cyber security.

Qualitative vs. Quantitative Risk Assessment

Qualitative risk assessment is a subjective weighting of the probability and level of impact of a potential cyber event. These values are typically communicated in a straight-forward "dashboard" fashion.

		Impact		
		Low	**Medium**	**High**
Probability	**Low**	Low Risk	Low Risk	Medium Risk
	Medium	Low Risk	Medium Risk	High Risk
	High	Medium Risk	High Risk	High Risk

There are two important advantages to qualitative risk assessments: they can be done quickly, and they are relatively easy to communicate. They also have two major disadvantages. Being subjective qualitative assessments are prone to natural biases that can make these assessments less accurate and less reliable. They also do not provide a concrete measure of possible impact upon which to weigh and base decisions, e.g. a high impact event is worse than medium, but by how much? What is the scale of low impact vs. high?

Enter quantitative risk assessment. Quantitative risk assessment (as the name implies) is based on metrics. These metrics culminate in a financial value for risk, and provide business executives – beyond IT and security professionals – with clear (defensible) criteria for making tough choices.

There are different flavors of quantitative risk assessment, but the common components are:

- SLE (Single Loss Expectancy): money expected to be lost if the incident occurs one time.
- ARO (Annual Rate of Occurrence): how many times in a one-year interval the incident is expected to occur.
- ALE (Annual Loss Expectancy): money expected to be lost in one year considering SLE and ARO (ALE = SLE * ARO). In quantitative risk analysis this is the risk value.

Besides providing metrics of loss, quantitative risk assessment attempts to give decision-makers more actionable intelligence on the future probability of an event by incorporating the recent history of similar events (within the ARO).

Of course one downside is quantitative assessments require more details, particularly better intelligence on the nature and potential impact of cyber threats. And at least initially, establishing a workable quantitative model can take longer than a subjective, qualitative assessment.

Changing Risks along the Continuum

Cyber-criminals and other bad actors, e.g. nation states, continue to develop tactics, techniques and procedures (TTPs) to enhance tried and true attack vectors as well as to exploit new, emerging vulnerabilities. Just as the enterprise has come to rely on broader, interconnected networks, the risks to any business has increased commensurately. The growing risks posed by advanced Distributed Denial of Service (DDoS) attacks is a good example. DDoS attacks aren't a new cyber threat. They have been around for almost 20 yrs. And the probability is that most organizations have some form of DDoS attack protection in place already. But, just as other cyber threats have evolved, so too have DDoS attacks. And thus should the continuum of reassessing the risk of DDoS attacks.

By any measure DDoS attacks have come a long way. The increasing frequency of contemporary DDoS attacks is not in question. Many organizations are under attack virtually all the time. Given the ease of acquiring and launching significant botnet attacks and the explosion in vulnerable Internet of Things (IoT) devices, there is no longer any peacetime from DDoS. But it is not only a question of frequency. According to NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report:

- Average DDoS attack sizes are now above 1Gbps, a key threshold in that an average attack can saturate the Internet connectivity of many enterprises.
- Low and slow, harder to detect application-layer attacks increased from 25 percent to 32 percent in 2017.
- 48 percent of the enterprises observed a multi-vector DDoS attack; up from 40 percent the previous year.

In reality, we have entered a new era of far more advanced DDoS. Advanced DDoS attacks are likely a planned, dynamic combination of multiple attack vectors. It could combine a state exhaustion (e.g., TCP-SYN attack), to cripple perimeter defenses, while at the same time deploy an application layer attack (e.g. SlowLoris), targeting a key customer service website. More and more, sophisticated advanced DDoS attacks are used as distractions or intrinsic parts of Advanced Persistent Threats (APTs) to cover up the downloading of stealthy malware.

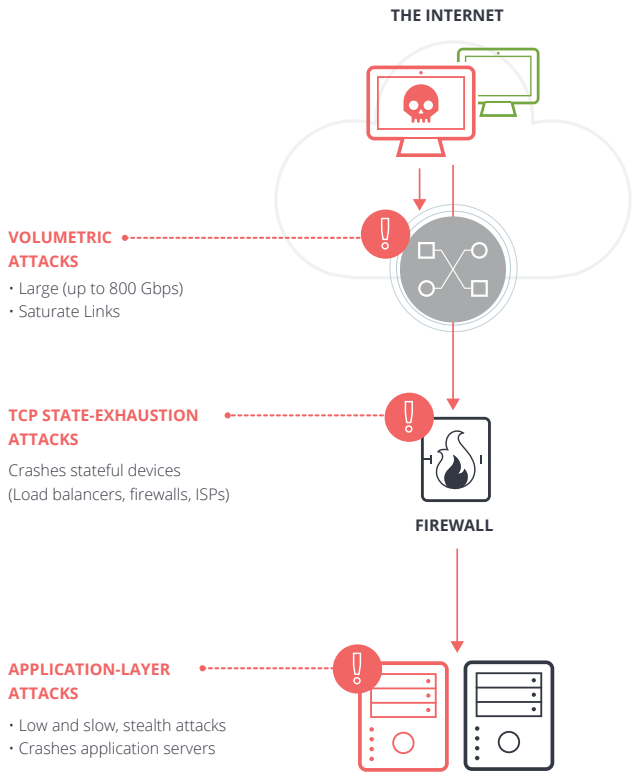

Figure 1: The modern-day DDoS is complex as it's a dynamic combination of 1) Volumetric, 2) TCP-State exhaustion and 3) Application layer attack vectors.

Just like APTs, compromised devices used for advanced DDoS attacks use outbound communications to report back (aka command and control or C2) to the threat actor and be instructed to adapt its Technique, Tactics and Procedures (TTPs). For example OMG, one of the newer advanced DDoS botnets is a variant of the Mirai Internet of Things (IoT) botnet used against Dyn in 2016. The OMG botnet is designed to scan for and infect IoT devices and launch attacks from within your own perimeter. This is a fundamental change and requires re-thinking advanced DDoS detection and defense, mainly regarding detecting and blocking outbound communications to know bad sites/actors and stopping internal DDoS attacks from occurring.

And let's not forget the costs. Respondents to NETSCOUT® Arbor's 14th annual Worldwide Infrastructure Security Report (WISR) reported business impacts due to DDoS attacks varied greatly in 2018. More respondents reported they observed very measurable attack consequences, such as the cost of specialized remediation and investigation services (39%), as well as increased OpEx and revenue loss (each at 38%). Damage to reputation/brand and increased insurance premiums were reported by 37%.

Measuring the Risks of Advanced DDoS

Established best practices for DDoS protection call for a layered, hybrid defense leveraging on-premise and upstream components. On-premise components (hardware or increasingly software) can detect and mitigate the "low and slow" application layer attacks more rapidly. Because of TCP-state exhaustion attacks, these stateless components should be placed at the edge of your network – in front of stateful next generation firewalls (NGFW), intrusion protection systems (IPS) or load balancers which are vulnerable to these types of DDoS attacks. NETSCOUT Arbor's WISR reported 54% of organizations had firewall or IPS devices experience failure or contribute to an outage during a DDoS attack.

Upstream protection from a service provider is the best and most cost-effective option against the larger, volumetric attacks, before they overwhelm your Internet connectivity. And for many organizations, leveraging the expertise of a managed security service provider for all the components makes economic sense. In other words, outsourcing some or all of your DDoS attack protection to experts who mitigate these attacks on a daily basis using the latest technology and best practices in defense can remove pressure on your already stressed out cyber security teams.

But even with layered protection, how can you measure the risk from advanced DDoS? On what do you base your DDoS protection decisions, and how do you communicate these decisions to management? If there is any upside to advanced DDoS it might be that much is known about DDoS trends and the TTPs of bad actors. This knowledge, coupled with the potential costs to a business, is the key to building a credible, quantitative advanced DDoS risk assessment.

Threat intelligence should be embedded in all layers of your advanced DDoS defense (and as much as possible provide automated alerts and mitigation). But more than that, specific contextual intelligence on likely targets/goals, recent activity, familiar TTPs and common modes of inbound AND outbound communications, helps IT management to understand the threat and help measure the risk.

There are different methodologies for quantitative risk assessment (see sidebar), but the three components described above are consistent. Conducting a quantitative risk analysis of DDoS attack make look something like this:

- Single Loss Expectancy: How much would it cost the business if your ecommerce site was down for 3 hours? Or key application server? Or customer service app? Contextual intelligence on specific, current advanced DDoS activity and threat vectors can help you focus on probable target business functions or applications, and therefore better estimate costs.
- Annual Rate of Occurrence: How times per year will this loss event occur? Are you an organization that experiences DDoS attacks on a daily basis, or is it more like 1-2 times per year? Look for industry stats, talk to your industry peers or reply upon your own experiences to help you determine the annual frequency of these attacks.

Factor Analysis of Information Risk (FAIR) is another quantitative risk analysis methodology. FAIR analysis first requires knowledge of the latest DDoS attack trends, in FAIR terminology, the Threat Capability (TCap). One compares those trends to the attack protection in place, known as the Resistance Strength. If the TCap of a DDoS attack is greater than the Resistance Strength, then the organization is vulnerable and at risk of loss.

- Annual Loss Expectancy: Once you have figures for the above you can derive a credible, annual risk value for each scenario, e.g. the risk value of a state exhaustion attack on the ecommerce site. This risk exposure value will be easily communicated to and understood by non-security executives.

Up to this point in your quantitative risk analysis you've approximated the potential loss using the "current state" of your DDoS attack protection (if there is any at all).

The next step in the analysis is to show how the loss exposure can be reduced by implementing a DDoS attack protection solution. It's one thing to see the reduction in risk exposure; but at what cost? In other words, how much is your organization willing to invest in protection to reduce the risk and ultimate loss?

This is where you can examine different DDoS attack protection options, their effectiveness in stopping DDoS attacks (and thus reducing the loss exposure) and their cost. For example, you could examine:

1. On-Premise DDoS attack protection only, managed by your staff.
2. In-Cloud DDoS Protection only, managed by a service provider.
3. A combination of on-premise and in-cloud DDoS protection, fully managed by a single service provider.

Now, presented with all this information, your/your decision makers can make a quantifiable assessment of the risk of DDoS attacks.

How granular and how frequently you re-assess risk depends on many factors: resources, type of and complexity of business infrastructure, perceived risks – not to mention appetite for risk. Quantitative and qualitative risk assessment approaches can be used together. Qualitative risk assessments based on your experiential knowledge can be used to quickly identify the most valuable and vulnerable assets, and then use quantitative assessment to narrow down specific risk scenarios and derive a value.

Progress along the Continuum of Risk

Risk management has become the basis for many enterprise security decisions. The majority of organizations recognize the continuum of cyber risk and the changing threats posed by advanced DDoS. It is encouraging to note, that according to NETSCOUT Arbor's 14th Annual WISR, 50% of enterprises reported that DDoS was a part of either their business or IT risk assessments. We are delighted to see that more and more organizations assessed DDoS risks on a recurring basis, either as an IT or business risk. According to the WISR, in 2018, only 7 % mentioned they do not consider DDoS in their recurring risk analysis process, a significant improvement over the 23 % reported in 2017. The ongoing assessment of risks along the continuum posed by advanced DDoS must be at the core of any effective cybersecurity strategy.

The growing threats from advanced DDoS require updated and in some cases quantified risk value assessments so as to implement the appropriate, cost-effective level of protection. Without a clear picture of the real, measureable risks from DDoS these decisions can be, well, especially risky. Given the scale and pace of the digital enterprise, quantifiable risk assessment may not be the only approach, but risk value measurements are key to making better decisions – and effectively communicating these decisions to all stakeholders.

FAIR Analysis – "How to Analyze and Reduce the Risk of DDoS Attacks"

https://www.netscout.com/sites/default/files/2018-07/SECWP_005_EN-1802-How-to-Analyze-and-Reduce-the-Risk-of-DDoS-Attacks_0.pdf

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECWP_009_EN-1901 06/2019