Is the *Internet of Things* becoming the *Internet of Risk*?

An analysis of the DynDNS DDOS and emerging IoT risk

Is the *Internet of Things* becoming the *Internet of Risk*?

An analysis of the DynDNS DDOS and emerging IoT risk

About Emergent

We help organizations “See Around the Corner” through a combination of professional services, and our Instinct Engine™ risk-quantification technology.

Through our products and services, you have a clear risk-based approach to find, assign responsibility for, and respond to cyber risks. We were established by leaders in the US Government and banking sectors to address today’s emerging Digital Risk Management challenges.

CONTACT
Emergent Network Defense
1133 15th Street, NW
12th Floor
Washington, DC 20005

SeeTheSwarm@endsecurity.com

Earl Crane, PhD
CEO, Co-Founder

Are you asking the right questions?

When we walk into an organization to assess their cybersecurity program or help them address a regulatory MRA, we start with one question;

What is your Cyber Risk Appetite?

This is a tough question every business leader now faces.

The reflexive answer to this question is always “none”, but that is too simplistic. The thoughtful answer is always “it depends”. The final answer is that risk appetite is nuanced and specific to your organization. Your statement of Cyber Risk Appetite should capture the business risks that are unique to your culture, values, technology, operations, and adversaries.

Let us share our five-step question model, and help you establish a Cyber Risk Appetite foundation for strong business today, tomorrow, and in the future.

Could *your* Internet of Things lead to an increase of your risk exposure?

Are you contributing to the Internet's botnet scourge?

Toward the end of October, as most people prepared for the Halloween onslaught of pint-sized goblins and superheroes, an army of pint-sized computers took down part of the Internet.

About 100,000 internet-connected devices—thermostats, baby monitors, and other "smart" devices embedded with the brains of a computer—compromised by malware, launched a distributed denial of service (DDOS) attack against Dyn, one of the premiere providers of Dynamic Name Services (DNS)—the equivalent of the Internet's phone book. Overloaded with fake requests, DynDNS servers were unable to provide legitimate services to their clients, like Amazon, The New York Times, and Twitter.

Internet of Things (IoT) botnets may be one of the biggest emerging Internet threats, and you should pay attention. Not because of the ability to launch crippling attacks to take out large sections of the Internet—as we saw the Dyn attack—but because your organization may be complicit in the attack.

What made this attack different?

This was not a large botnet, though it could be a preview of the magnitude of what's to come. The Dyn DDOS had only about 100,000 bots, while today's largest botnets to date approach the tens of millions[1].

There are currently about 2 billion internet connected computers, and a conservative estimate of traditional botnets is that one-half of a percent of internet-connected devices will fall into a botnet.

However, there are currently an estimated 22.9 billion internet-connected devices—estimated to grow to 50 billion by 2020. This means that IoT DDOS attacks like the one that impacted Dyn have room to grow. We are at the beginning of a new wave of enormous botnets of the future.

An IoT botnet in 2020 could have upwards of 250 million infected devices, or almost 10% of today's connected computers. This will make the Dyn attack look quaint when compared to the challenges we could face in just a few years.

Why should I care? I run a secure enterprise, and we don't have IoT?

Even if you do not have IoT deployed in your enterprise today, you likely will in the next few years.

Enterprise adoption of IoT devices—including commercial and government—will account for almost 80% of IoT adoption. This will be one of the largest attack surfaces for your enterprise and an intrusion vector possibly eclipsing phishing email as a top risk exposure[2].

If your organization has difficulty managing traditional enterprise IT risk today—servers, workstations, mobile devices, and even a cloud deployment—the wave of IoT devices will be larger by an order of magnitude (10 times larger). That is an unmanageable attack surface expansion for almost every organization operating today, and this is the greatest risk to enterprise IT risk managers as they absorb the impact of future IoT DDOS attacks[3].

Who is responsible for risk management of connected devices?

For IoT devices deployed at home—unmanaged devices—the answer today is not clear; it may be the consumer, the manufacturer, or the internet service

provider. However, responsibility for enterprise IoT devices is very clear; the company responsible for installation and maintenance of the IoT device is responsible for safety and security.

Within the enterprise, the responsible party may come as a surprise. Most organizations today operate in a digital corporate ecosystem, and the introduction of IoT devices brings real-world physical realities into this digital corporate ecosystem. Building safety and environmental systems, manufacturing quality control systems, HR and healthcare systems, logistics and GPS systems, and field monitoring systems all are becoming components within the enterprise digital corporate ecosystem. Essential operations of this industrial-connected-IoT (IIoT) is a risk beyond scope of traditional IT systems.

Safe and secure operation of these systems captures executive and board attention, and many leading organizations have identified this risk as an existential threat to their organizational competitiveness and survival. Leading organizations have designated a Chief Risk Officer, or Digital Risk Officer—sometimes as a direct report to the CEO, or sometimes under the Chief Legal Officer. Clearly, this responsibility does not fall just under the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO).

What is the first step to protect myself?

Can you quickly take a survey of your digital assets that matter most, and ensure their safety and security? How are you managing your digital risks today to ensure your enterprise IT is not part of a botnet, or worse, an intrusion vector to compromise your organization? Have you assessed the risks if you are on the sending side of an attack? What are the risks if you are one of the attackers, rather than the one being attacked?

Most importantly, have you assessed your digital risk exposure to health, life, safety and operational capabilities for your company and employees?

If you can't readily answer these questions now, how will you answer to your executive board or your regulators?

The first step in getting a handle on emerging risks is to properly identify today's digital risks, then develop and clearly communicate your appetite for loss. This Cyber Risk Appetite exercise will prepare you to answer critical IoT questions later.

You can answer these questions with a simple four-step process:

1. Identify what matters most, from a business perspective
2. Identify how digital risks can impact what matters most to your organizational success
3. Identify cybersecurity knowledge and practices to ensure appropriate protection of your digital assets
4. Instrument your environment to collect data about your digital risks, and make ongoing informed risk-based decisions.

Once you have a handle on the above Risk Management process, you will be better-equipped for today's—and tomorrows—Digital Risks.

As you adopt more IoT, have the following conversations with your business and IT stakeholders:

1. Ask "How many IoT devices should we have?" and "What is their purpose?"
2. Scan/monitor your network for new IoT devices. How do they add up to your expectations?
3. Identify the major risks to your operations from unmanaged IoT devices
4. Ask in-house or external subject matter experts how big/bad a risk impact from your newly-discovered IoT devices could be, and compare that to your Cyber Risk Appetite.
5. Estimate a dollar-based impact using a risk-based approach to translate the digital risk impact into business action for your executives.

Get Started today!

We can help with this very important move into Digital Risk Management.

Contact Emergent Network Defense for information on how we can get these conversations started within your organization.

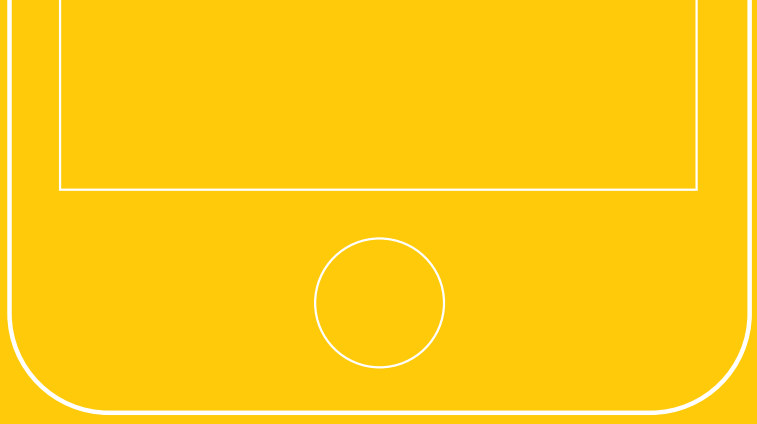
We can help you discover, develop, and communicate your Cyber Risk Appetite, as a first step in preparing for tomorrow's emerging digital risks.

Email us at *SeeTheSwarm@endsecurity.com*

[1]: http://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage

[2]: http://www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-2

[3]: http://blogs.rsa.com/dyn-ddos-attack-how-iot-can-take-down-the-global-information-grid-backbone-part-ii



EMERGENT

1133 15th Street, NW
Floor 12
Washington, DC 20005

www.endsecurity.com