DDoS Challenges and Mitigation

Improving the Security, Availability, and Success of the Connected World with Real-time, Always on DDoS Mitigation Services

Contents

Introduction

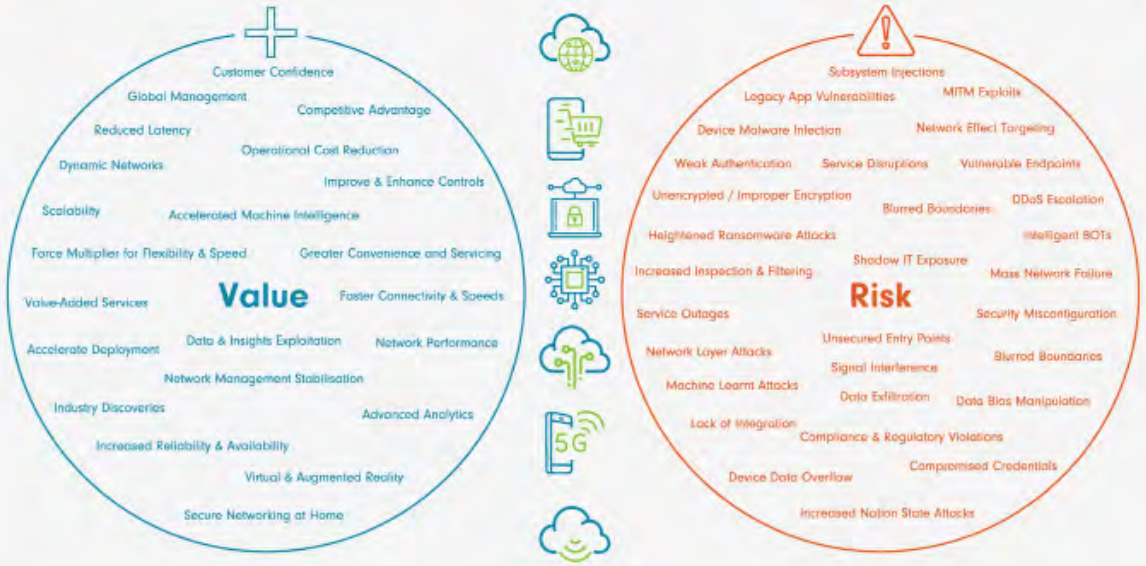
With new technologies such as 5G and IoT, the increased adoption of cloud, edge and software-defined architectures and the explosion in digital applications, the risk environment has grown more perilous and costly as everyone embraces an interconnected world.

Today the business landscape encompasses globalized supply chains, complex financial interdependencies, and immediacy of action related to consumer principles. This requires businesses to challenge the value and risks of innovation (Figure 1).

Many executives remain fixated on the demonstrable value of their strategy and performance management, often failing to challenge competencies or strategic decisions from a risk perspective.

FIGURE 1

The value and associated risks of new technologies



Source: SynergySix/Omnisperience

Digital transformation has required many operational models to evolve over the past two to three years. New technologies that increase connectivity, automation and intelligent decision-making are replacing historical systems and consumer interactions.

Consumer digital expectations during the global event in the first half 2020 disrupted traditional cyclical business evolution planning, increasing operational complexity for bringing consumers and businesses closer together. These advancements have required business leaders to evaluate the value-to-complexity-to-risk ratio, and any exposure across their ecosystem, at a pace that challenges even the best strategists.

Assessing the value-to-complexity-to-risk ratio is traditionally based on the known likelihood and impact via the implementation of an Enterprise Risk Management (ERM) framework. Businesses must prioritize the ability to respond to emerging risks, something that occurs daily within the cybersecurity arena. Cybersecurity aligns to the highly likely, high-impact events on which risk management should focus most of its attention. Threat events can emerge with disarming velocity and immediacy of impact, taking unaware companies by surprise.

Mature (incumbent) organizations are transitioning to a 'digital-first' engagement strategy, creating an equilibrium of digital effectiveness alongside new entrants that have digital at their core. This has accelerated the opportunity for organized cybercrime groups and lone hackers to unleash their cache of malware and data breach exploits. Many of these cybersecurity exposures are summarized in Table 1.

TABLE 1

Innovation Value Risk Table

Innovation	Description	Value	Use Cases	Risk
Edge Computing	Data collection, processing and reporting closer to the end user	• Exploit data and insights faster • Compute data closer to source • Creates competitive advantage	Enterprise data centre, healthcare, smart cities, and more	Distributing data across networks containing numerous (100s-1000s) devices and data centres operating far from a company's main locations can create problems with network visibility and control.
Internet of Things (IoT)	Sensors capture data and embedded connectivity to exchange information over a network.	Business insights and opportunities, reducing operational costs and creating value-added services.	Home devices, personal assistants, smart meters, smart security, connected cars, inventory trackers and many more	IoT devices can be rendered inoperable or have their performance influenced. They have inadequate security and can easily be harnessed in to botnets to launch large-scale DDoS attacks on other targets
Digital Applications	Deliver specific value for businesses, consumers and citizens via marketplaces, cloud services and portals	"What ever you need, there is an app for it." Driving accessibility, speed, efficiency and performance at costs that are not prohibitive and always with a 'user-first' purpose	Every industry, market size, person, persona, social experience, engagement, everything, everywhere.	Digital applications exist in the cloud. This exposes users to cloud security risks and a lack of 'security-by-design' hardening. Shadow Apps are not configured against a security framework of 'risk-mitigation' which opens the entire business to cyber attacks.
Software Defined Networks (SD-WAN)	Allows software-defined policies and business intent to WAN connections such as MPLS, 4G, LTE and broadband internet services	Provides centralised management, bandwidth management, some cost control and some networking visibility	• Deploy multiple links • Simplify/accelerate/secure branch deployment • Access to IaaS and SaaS • Global managed WAN	Traffic moves outside the bounds of the data centre perimeter that could place users in remote locations at risk as SD-WAN doesn't automatically integrate with the existing security infrastructure. 'One unsecured entry point is all that's needed for a breach to occur'
5G	A new global wireless standard that enables a new kind of network that is designed to serve consumers and digitalisation of industries.	Faster speeds and lower latency, enables new business applications and connectivity opportunities to realise their full potential.	Five key functional drivers: superfast broadband, ultra-reliable low latency communication, massive machine-type communications, high reliability/availability, and efficient energy usage.	Based on software, 5G expands the risks related to major security flaws. Emerging techniques, network slicing, network functions virtualization (NFV) etc blurring their boundaries and increasing the risk of high-powered DDoS attacks sourced from 5G-enabled devices and botnets made up from them. All outbound service providers now have a serious risk of inside-out attacks.
Virtual Private Network (VPN)	A secure medium within the public internet forming a tunnel between the sender and receiver for sharing sensitive data.	Computer acts as if it's on the same local network as the VPN, conveying network traffic over a secure connection. Allows you to securely access local network resources wherever you are the world.	Connectivity and secure access allowing the authorised user to access a business network while travelling, ensuring the local resources are not exposed directly to the internet, maintaining user and business security policies.	The remote machines using VPN must themselves be secured from abuse, requiring the enforcement of certain minimum standards with regards to operating system, antivirus software, firewalls and so on. If the target corporate network is compromised with a DDoS attack, no access can be granted to the VPN and the user is prevented from getting to their corporate data and systems.
Artificial Intelligence (AI)	An interdisciplinary science with multiple approaches concerned with building smart machines capable of performing tasks that typically require human intelligence.	Artificial Intelligence (AI) underpinned by Machine Learning and Deep Learning can observe, analyse and learn from data and mistakes just like our human brains can	Significant breakthroughs in healthcare, physics, manufacturing, finance, and retail. Also the enhancement of autonomous cars, AI-powered plagiarism detectors, neural networks to detect fraudulent transactions, cybersecurity threat detection and product recommendations.	Adversaries can learn how to systematically feed disinformation to AI powered device software opening a new attack vector based on this vulnerability. Cybercriminals use machine-learning to detect and bypass security detection systems. A combination of malicious actors and AI technology could be a deadly combination across networks, applications and communications.
Cloud	On-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.	Companies of all sizes - where the reliance on internet connectivity for access and multi-tenant infrastructure balances the playing field - embracing cloud as a force multiplier for flexibility and speed.	An alternative to existing compute infrastructure by providing on-demand and 'as-a-service' (scalability, elasticity, etc). It will continue to exist and widen its value alongside traditional data centres and the new Edge / SASE / SD-Branch computing architectures.	Cloud is not necessarily better or [could be] worse than an on-premise data centre for the risks that its infrastructure could introduce, such as: Loss of data and intellectual property, compliance violations and regulatory actions, service outages due to DDoS attacks and injection techniques.

Source: SynergySix/Omniperience

A defensive or reactive approach to risks appears to be standard practice with engagement only happening after the event. The result is that executives needlessly endanger their company, employees and customers to the devastating effects of cyber risk, while personally taking on higher legal and reputation liabilities.

The most advantageous mitigation against any risk is real-time decision-making that can help to action a halt before the business is impacted. In ERM there are certain known risks; economic factors, natural factors, and political factors that cannot be internally mitigated in real-time. A majority of the reporting tools used for risk management continue to be built for control processes around retrospective data and analytics. These are excellent for operational processes, procedures and governance but do nothing for high-impact cybersecurity risks that need to be mitigated with proactive and real-time controls.

Appropriate technical and skilled resources are a critical factor in successful risk governance. Companies usually devote most of their risk and control resources in sector-specific areas such as macro-economics, supply chain and health and safety. The same companies can, as a result, fail to provide sufficient resources to monitor other highly significant risks such as cyber-attacks. The introduction of a culture that embraces cyber risks - as well as the traditional sector-specific areas - will reinforce strong risk management practices.

Real-time risk control operations enable immediate analysis of prevented cyber-incidents, with empirical data to understand the root cause of an intended attack. The 'real-data' from such approaches can also be used to evaluate and further harden existing systems and controls, to demonstrably lessen future risks and maintain a closer equilibrium with the cyber criminals.

Network Effect Encourages Dependencies Across Your Community

The co-inventor of the Ethernet, Robert Metcalfe also gave us the eponymous Metcalfe's Law which describes the intrinsic value of a telecommunications network. It has since been popularized as "The Network Effect" by economists and technologists.

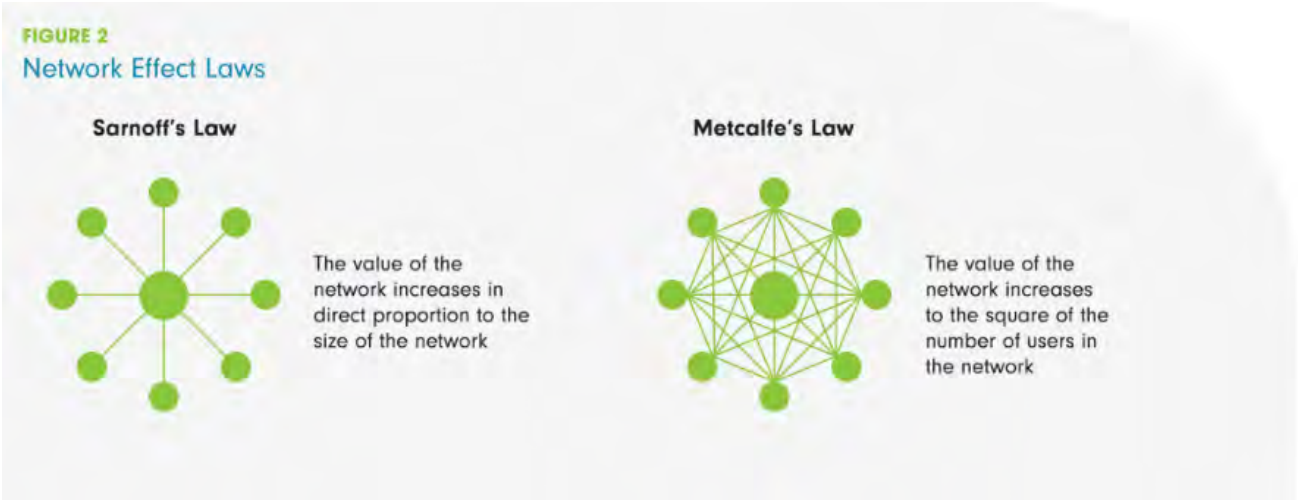
Network Effect exists when the addition of another element [to the network] makes all the existing elements in it better off. It's a positive feedback loop. As the network grows, the more value it provides. The more value it [the network] provides, the bigger it grows. It's the economics of having an extra point on the network and that you can build a lot more services on the existing network, thereby expanding its power. A 'Network Effect' typically accounts for 70% of the value of digital-first companies. These types of organizations are digitally minded from the outset with the idea of an interconnected, online and physical experience that is user-centric.

Sarnoff's Law (seen as Metcalfe's predecessor) is contingent on growing the size of network, whereas Metcalfe argues that the [real] value of the network is proportional to the square of the number of users. Or, in other words, the value was due to the connectivity between users enabling them to work together and achieve more than they could alone.

A Network Effect implicitly refers to having a global benefit wherein each new user benefits the entire network. However, in practice, network effects are local and clustered into subset or micro-networks within the larger network. These effects can and are being extended as multiple local/clustered and global individual networks are interconnected with authorized connections. See Figure 2.

There are many varieties of Network Effect depending on the type of businesses and individual or cross industry use cases, each with their own strengths and weaknesses. In addition, each use case can exploit one or [many] more network effects.

FIGURE 2
Network Effect Laws



Direct Network Effects

Direct (same-side, or symmetric) network effects happen when an increase in users directly creates more utility for all of the users, resulting in a better product or service.

Direct Network Effects	Description
Physical	Infrastructure, typically utilities (e.g. Telecoms, Railroads, Electricity)
Protocol	A common standard for operating (e.g. Ethernet, Bitcoin, MPEG-DASH)
Personal Utility	Built on personal identities (e.g. WhatsApp, Slack, WeChat)
Personal	Built on personal reputation (e.g. Tik-Tok, Facebook, Instagram)
Market Network	Adds purpose and transactions (e.g. Houzz, AngelList)

Indirect Network Effects

Indirect (cross-side, or asymmetric) network effects happen when an increase in users indirectly creates more utility for other types of users.

Direct Network Effects	Description
Marketplace	Enables exchanges via buyers & sellers (e.g. eBay, Gumtree, Amazon)
Platform	Adds value to the exchange of a marketplace (e.g. iOS, Nintendo, Minecraft)
Asymptotic Marketplace	Effect depends on scale (e.g. Uber OpenTable, TripAdvisor)
Data	Data generated through use enhances utility (e.g. Google, Waze, IMDB)
Tech Performance	Service gets better with more users (e.g. BitTorrent, Blockchain)
Language	A brand name defines a market or activity (e.g. Google, Uber, Zoom)
Belief	Network grows based on a shared belief (e.g. stock market, religions)
Bandwagon	Driven by social pressure of fear of missing out (e.g. Apple, Tesla)

Technology Continues to Harness the Power of Network Effects

The digital economy thrives on interconnectivity. As the Network Effect expands, the user is capable of extending their reach in the digital world, realizing the full experience that software and communication providers are promising.

To help ensure the success of each user, security service providers need to:

- Deliver a product that creates a differentiated and unique value proposition to all users
- Integrate with cross-industry partners that enhance your offering
- Plan and execute an effective user-centric and led business model
- Increase the economies of scale on both the supply and demand side solving their unmet needs
- Retain customers with a product and experience that is 24/7
- Continue to deploy the latest innovation to defeat the competition
- Strive for operational excellence by automating stability, growth, and engagement

Ecommerce Market Opportunity

The ecommerce market grows every day. Currently there are more than 1.9 billion citizens globally that are changing their purchasing behaviors thanks to their engagement with digital platforms. It is anticipated that citizens, globally, will spend in excess of $11.9 billion online during 2020 from an overall $418 billion market opportunity (online and in-store). That's a conversion rate of 2.86% with each transaction averaging $220.

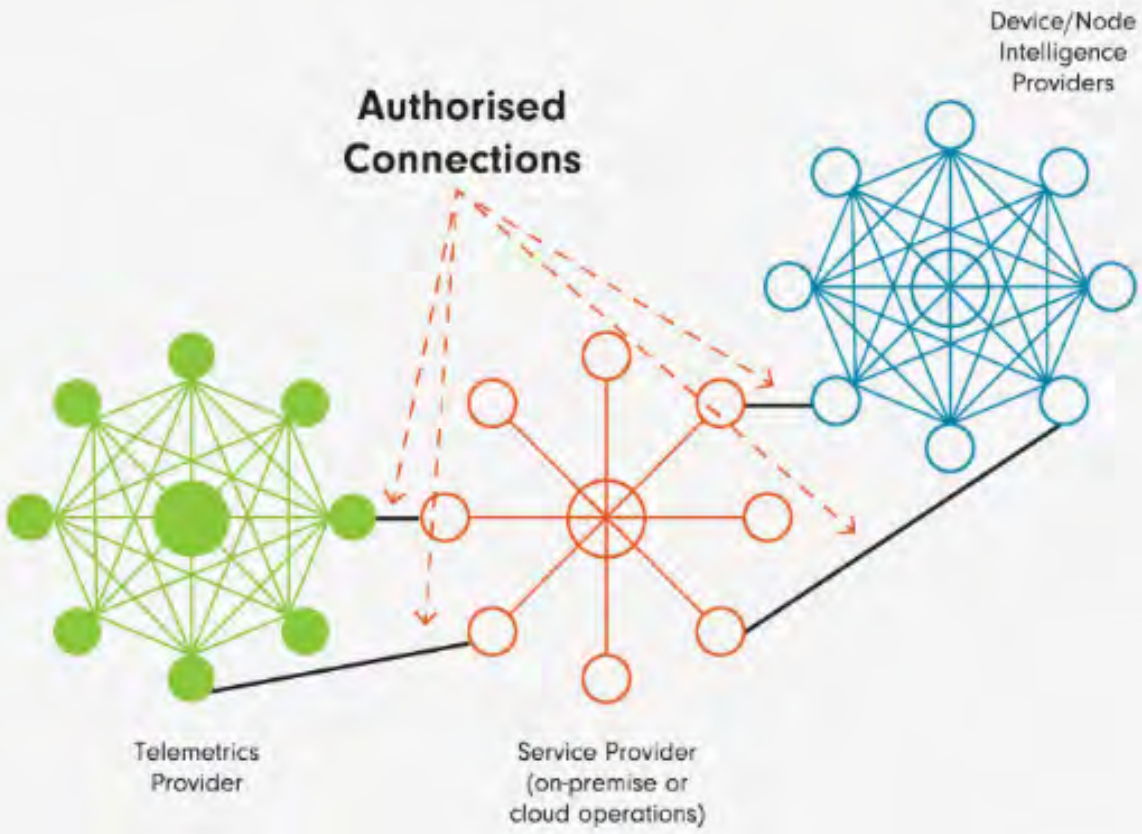
How Telematics Aids the Network Effect: A Real World Example

Telematics for supply chain and business systems includes a variety of vehicular-based data (GPS, ELD, IoT, etc.). Commonly used for GPS tracking and satellite navigation it has now enabled many other applications, including car sharing, enhanced road safety and emergency warnings. This is a clear example of a mixed network effect (see Figure 3), exploiting direct physical and protocol networks as well as indirect data and tech performance networks. If you add in AI (artificial intelligence) technology, in the form of intelligent agents, you now have a system that can peer into the future. It considers all the factors such as speed, traffic and delivery times to alert you to potential problems well in advance.

Intelligent agents can go further than just alerting you to any issues. The use of AI can help to formulate contingency plans that maximize service levels at the lowest cost. Intelligent agents can also automate logistics solutions (such as change dock door appointments, create and change orders, or expedite shipments) to keep service levels high and your supply chain running smoothly. Now you have visibility of "what and who is where" for the vehicle, the driver (and any passengers), the container, its contents, its route and the receiving customer. This type of value – enabled by telemetrics - can help to realize the impact that delays may have on a business.

FIGURE 3

Interconnection of local/global networks



An example of how Metcalfe's law and Sarnoff's law can integrate across different types of business network infrastructures.

Challenges

The Network Effect benefits for telematics take advantage of the relationship between

1) multiple nodes/users,
2) the availability of communication networks and protocols, and
3) the willingness of the user (consumer & business) to take advantage of the data to increase their experience.

These three advantages can also become risks across the operational collaborative network, as below.

1

The critical success factor across the entire operation is connectivity. Without the ability for the nodes (cars, containers, traffic systems, office platforms, IoT devices, source location, target location, etc.) to "talk to each other", they become isolated from intelligence and ineffective. Partial or full network unavailability means the user-experience is at risk due to the many critical elements they are relying on.

2

The intelligence is rich and of immense value due to its near- or real-time nature. It requires a continuous flow of new data to maintain that value. The lack of all or some of this data, including the manipulation of that data (bias), as a result of cybercriminal activity can cause the user to make incorrect or uninformed decisions. These could delay the departure/arrival resulting in goods being sent to the wrong location or the damage of perishable goods in cold chains (due to cyber interference instructing the refrigeration units to turn themselves off).

3

Both the intentional and unintended growth of the network effect has major benefits as organizations adopt a more digital-first approach to their business operations. The primary asset that network effects exploit is the value that the data being transported can provide to individuals and businesses.

Organizations that hold the various classifications of data as the differentiator in their business need to acknowledge that this data - and the growth in network connections needed to reach the point of usable value (user/business/ device) - can also be a risk to every person and node across the network [effect].

Cybercriminals have the capability to intentionally disable, or inject malware into, communication networks to influence your operations and apply a negative network effect for their own purposes.

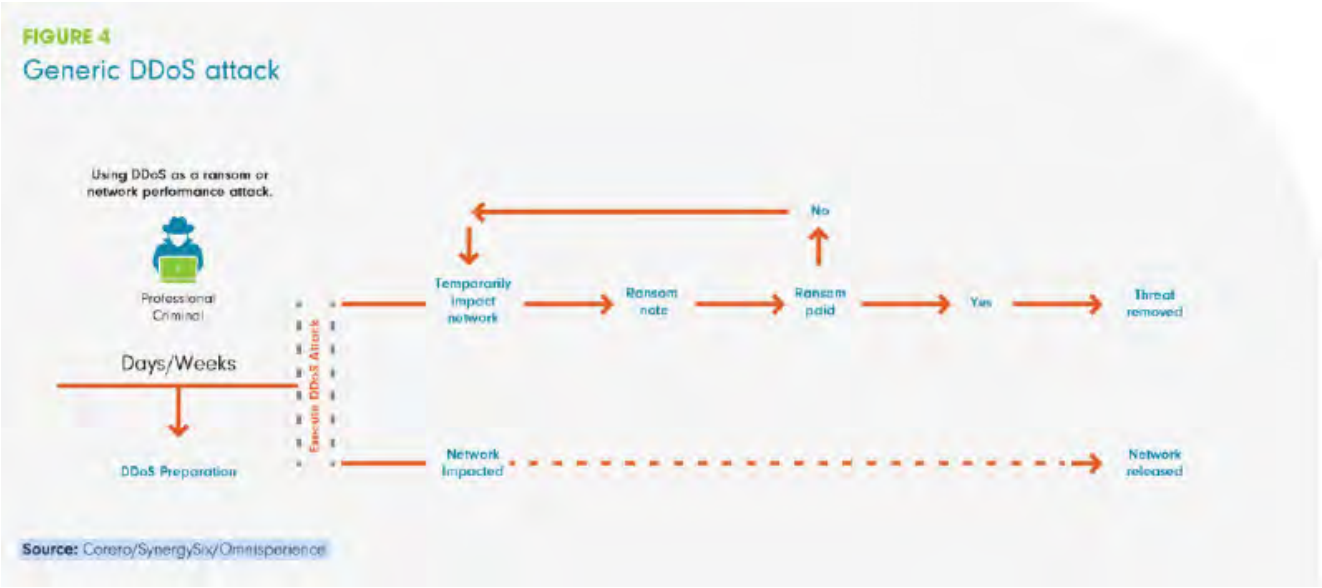
How DDoS Attacks Directly Impact the Lives of Individuals and Businesses

Distributed Denial of Service (DDoS) attacks are not an expensive outlay for cybercriminals. A mid-sized attack that lasts for a whole day can be bought for around $250 on the dark web. This amount of money is insignificant to the cybercriminal in comparison to the damage to the targeted businesses and its customers when the service they are expected to deliver or receive becomes unavailable.

What is a DDoS Attack?

The definition of a Distributed Denial of Service (DDoS) attack is where many compromised systems attack a single target, causing a flood of incoming messages which overwhelms the system, causing it to shut down or become unresponsive (see Figure 4). This is distinct from a Denial of Service (DoS) attack which typically involves a much lower rate of traffic, sourced from a single device.

FIGURE 4
Generic DDoS attack



Why do Cybercriminals Use DDoS?

When DDoS attacks turn into incidents they are instantly devastating to the target. If you understand the mindset of the cybercriminals, disgruntled employee or unhappy customer, they are typically trying to achieve any one or more of three objectives:

1

Disruption:
The network and connected services are at the core of business operations. The perpetrator may be trying to make a social or political statement by shutting down a specific website or large portions of the internet. Alternatively, an unscrupulous competitor may be looking to gain a competitive edge, by causing intermittent or protracted outages.

2

Currency:
The cybercriminal will be viewing currency directly and indirectly. Direct currency is achieved where professional 'hackers for hire', Script Kiddies and organized criminal groups (OCG) will use DDoS to extort differing values of immediate payment, in the form of a ransom demand. Alternatively, they may be focused on the indirect currency that results from damaging the longer-term viability of the organization due to the impact they are able to cause on customer purchases, plus the remediation and compensation payments that are often incurred.

3

Data:
DDoS itself cannot be used as a direct data exfiltration tool but it can be very effective as a diversionary tactic. This is when the cybercriminal can execute a parallel attack that could initiate a data breach or wipe/lock data for a ransom, exploiting proprietary, personal, or customer information for future exploitation. See Table 2 to realize the average cost of a data breach for differing sized organizations and industries.

TABLE 2
Average cost per data breach

Liquid Damage	Disasters	Software Corruption	Hard Drive Formatting	Hackers & Insiders
Human Error	Viruses & Malware	Hard Drive Damage	Power Outages	Computer Theft

Size of Company	Less than 500	500-1,000	1,0001 – 5,000	5,001 – 10,000	10,001 – 25,000	25,001 +	Cross Industry
Average cost per Data Breach	$2.35 million	$2.53 million	$3.78 million	$4.72 million	$4.61 million	$4.25 million	$3.86 million

Industry	Public	Retail	Average	Services	Pharma	Energy	Healthcare
Average cost per Data Breach	$1.08 million	$2.01 million	$3.86 million	$4.23 million	$5.06 million	$6.39 million	$7.13 million

Source: 2020 Verizon Data Breach Investigations Report (VDBIR)

The direct financial costs may not be the only attributable impact on your company from a DDoS incident. There are other tangible effects that could have a far more severe impact in the long run.

Financial Loss:
Estimates are calculated at ~$218k as the average cost of a DDoS attack (without any additional distraction attacks), that amounts to $10 billion in the US in one year. Heavy internet-trafficked sites such as e-commerce, gaming, and web hosting sites are in the spotlight and can lose hundreds of thousands of dollars for every minute their sites are down.

Remediation and Compensatory Costs:
All organizations, revenue-dependent or not, will have some amount of remediation costs. Some organizations, such as web hosting providers whose outage affects thousands of its own customers, might have significant compensatory costs to pay.

Loss of Customers and Loss of Customer Confidence:
In a world where any conceivable product is available to purchase with just a few mouse clicks, loss of online customers can be fatal. When customers abandon a poorly performing or unreachable site, the loss isn't just in immediate revenue, it's the potential loss of loyal customers who may go to a competitor's site and never return. Figure 5 below demonstrates the loss of customers, revenues (new and returning) when an ecommerce platform is not available or is performing poorly.

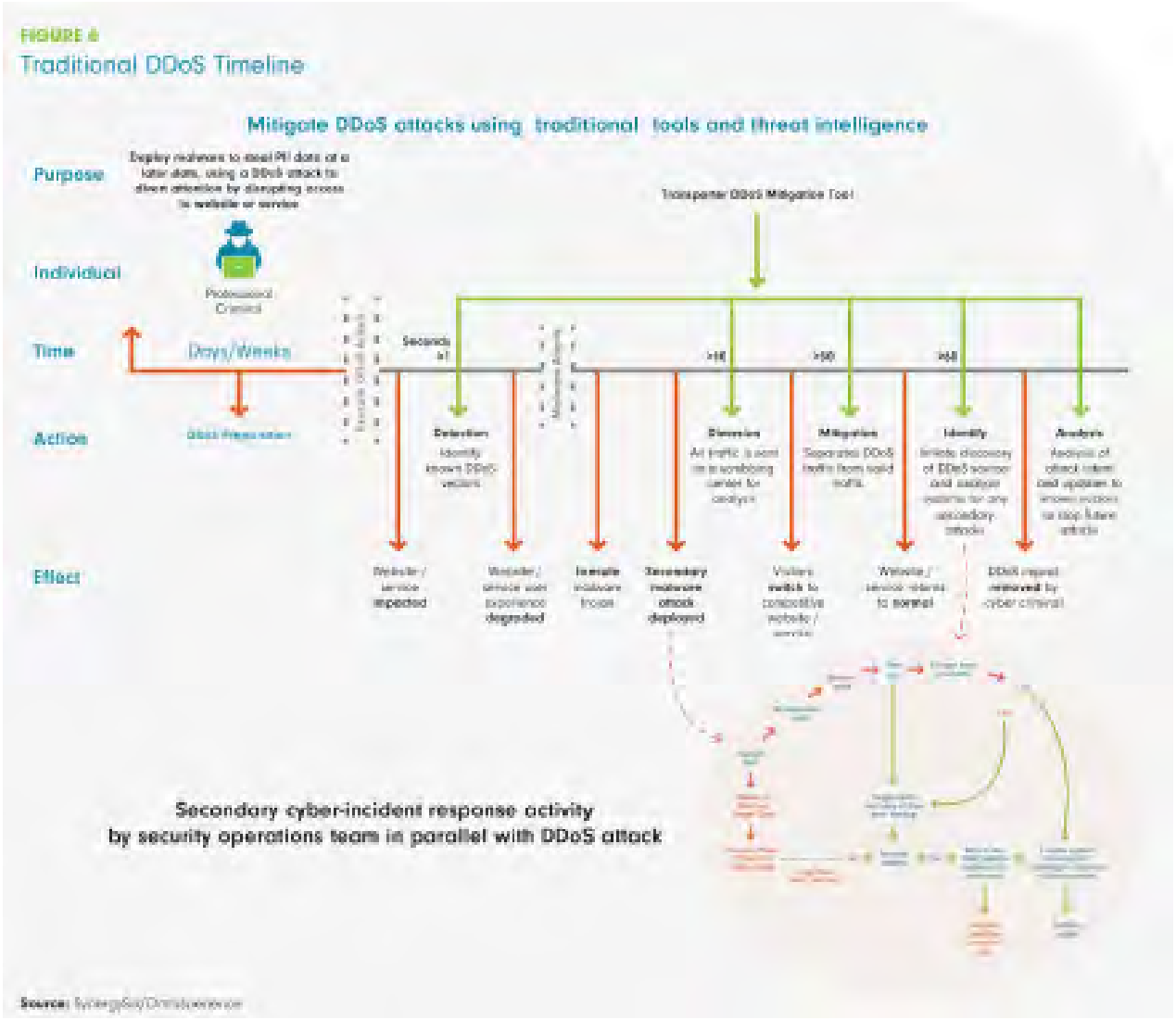
Reputation and Goodwill:
No business wants to make headlines for its security failures. Customers are especially less forgiving with businesses like banks and credit bureaus for whom trust is an important factor. It can take time for some businesses to repair their reputation and brand after a DDoS attack, especially if the attack is used as a diversion for a data breach in which personal or customer data is stolen or compromised.

Threat of Legal Action:
Organizations that have been the victim of DDoS attacks would rarely be challenged with legal action from consumers due to a number of practical issues, such as tracing the perpetrators of the attack (which is further compounded if the perpetrator's country of residence does not have computer misuse legislation) as the cost to prove it may be high. Whereas organizations might be more held to account by business customers with service level agreements (SLAs). If you are a cloud or web service provider - a lack of service can cause hundreds of thousands of other companies' websites to go down.

[Lack of] Engagement Effect

The devastating effects of a DDoS incident strangles the target organization and its users/ customers. The majority of communication platforms (phone, email, apps) used will also likely be blocked. This limits the capability for the organization, its partners and more importantly its customers' ability to understand why the service is not available.

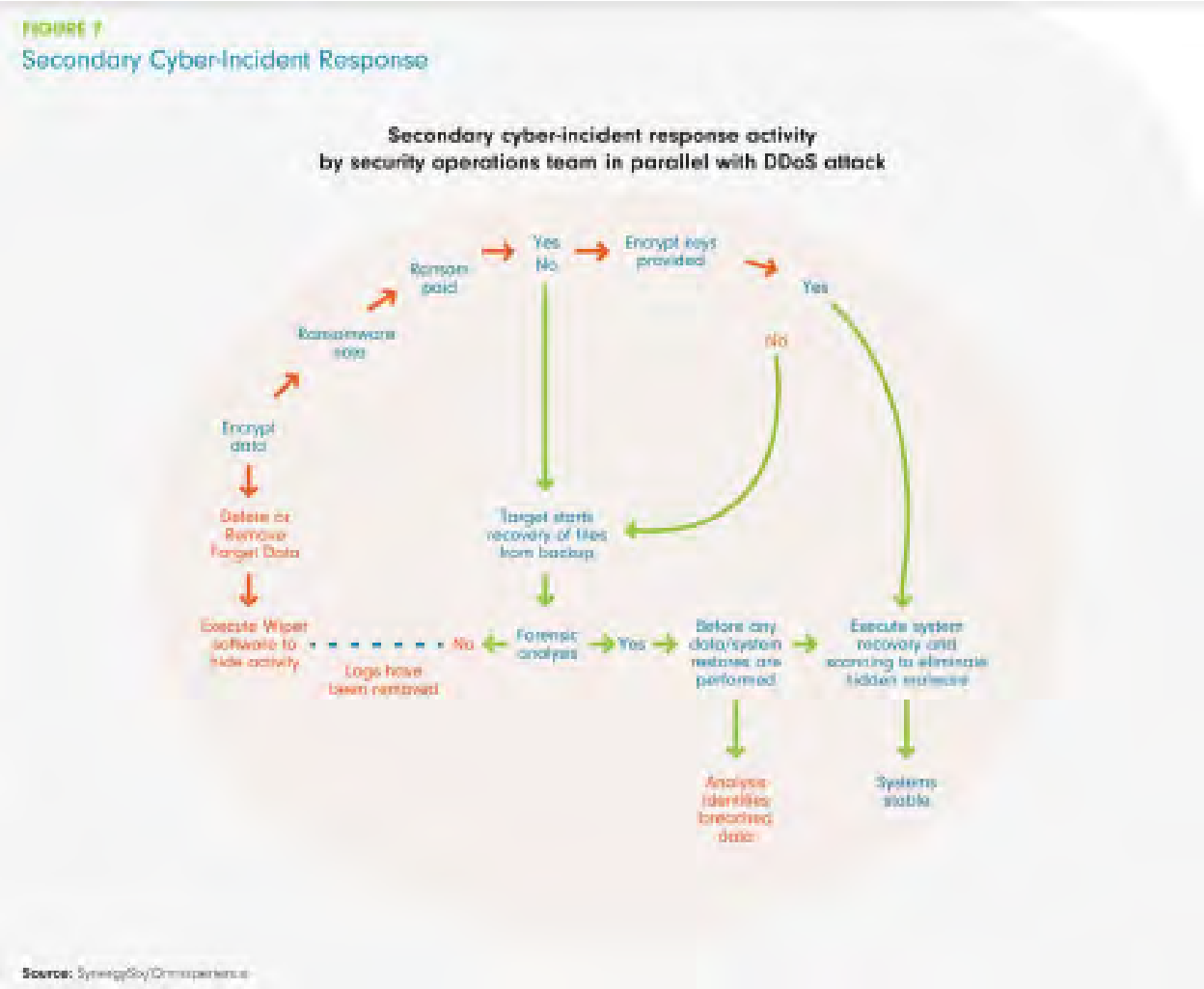
The majority of DDoS attacks encountered will have more than one attack vector. Figure 6 shows a timeline of a diversionary DDoS attack activity leading up to, during, and after the incident. The example is for a DDoS attack combined with malware deployment to encrypt data for the purpose of extracting a ransom payment.



If the DDoS attack is not instantly remediated by the DDoS protection tool it becomes a DDoS incident. This requires engagement by the IT or security administrators and scrubbing centers that immediately extend the outage by having to contact third party specialists to help resolve the issue due to lack of in-house specialist skills. Any outage of more than a couple of seconds will be picked up by consumers and its effect amplified as news spreads via social media channels. This increases the coverage, can impact a company's reputation and open the door for business competitors to start offering alternative services.

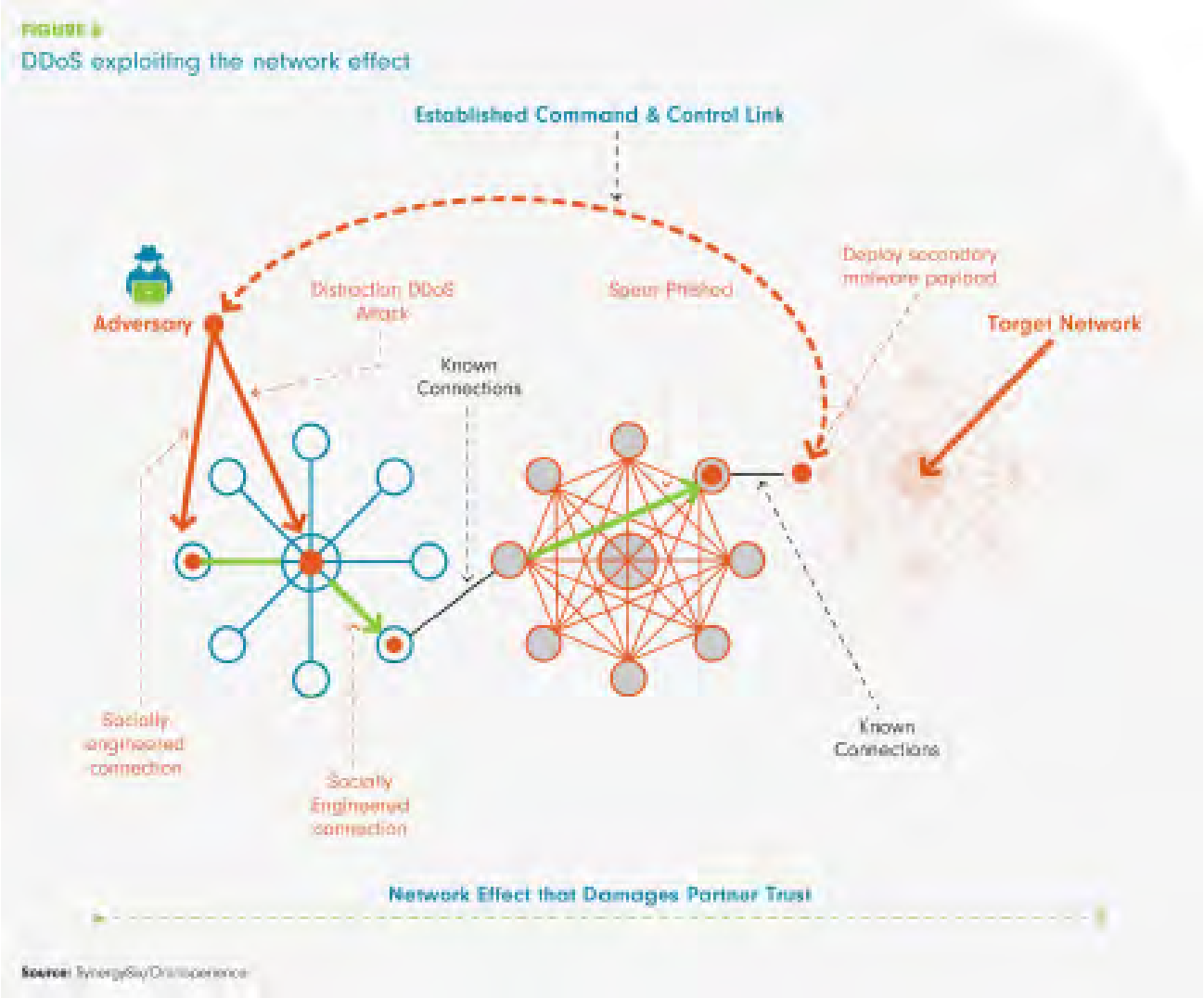
The lack of immediate DDoS mitigation creates a performance degradation on the network. This is the opportunity for the attacker to execute a secondary malware deployment (see bubble & Figure 7). The IT or security administrator's urgency to mitigate the DDoS attack increases when the attacker sends a ransom note notifying the company that they have also encrypted sensitive data. What should be the priority for the security analyst when this happens? To prioritize network performance to resume user/visitor confidence, find the encrypted data and any possible exfiltration, or start recovery from read-only snapshots of the encrypted data?

FIGURE 7
Secondary Cyber-Incident Response



DDoS in Our Connected World

We have already outlined how our connected world, encouraged by the Network Effect allows everything and everyone to source, connect and engage wherever and whenever we expect. Digital networks connect the world and enabled the growth of diverse working place practices – as experienced in 2020. Businesses are becoming more and more dependent on critical applications including any channels used to communicate, generate contracts, sell goods or any other service directly impacting the bottom line. Figure 8 shows the dependency on those network effects and provides an overview of the stages executed via authorized gateways for cybercriminals to reach critical partners or target stakeholders across supply and value chains to establish an ongoing command and control link.



Industry Impact from DDoS

Looking at the practicalities of our digital lives today we can see how a sustained DDoS attack could reduce individual productivity, loss of revenue, and more broadly impact our economy. Every second counts to digital-first businesses. One in every two people you see around you is connected to the internet and one in three people shop online. If their experience is disrupted, then business productivity - as well as current and future revenues - can all be instantaneously impacted. Table 3 provides a guide to the actual revenue impact of an extended DDoS incident, whether you are a leader (1% market share) or a breakthrough provider (0.1% market share).

TABLE 3

Every Second Will Cost Your Business

Time to Mitigate	Definition	Effective TTM	Why	Impact Cost (1% market share)		Impact Cost (0.1% market share)	
				Existing Client	New Client	Existing Client	New Client
Real-Time	That time-to-mitigation being short enough that there is no perceivable impact on the target as a result of a DDoS attack	Immediate	No Customer Impact - inline real-time automation without scrubbing centers	None	None	None	None
>0 seconds	The deployment of known attack vectors that are immediately mitigated and do not cause an incident to be analysed	Immediate	No Customer Impact - All mitigated attacks are known and pre-built into policies	N/A	N/A	N/A	N/A
>5 seconds	Defined service level agreement using automated mitigation, assuming mixture of known and unknown attacks	5+ seconds	Includes time for redirect to scrubbing centers, analysis and mitigation.	$8 million repeat sales	$49 million opportunity to convert	**>$8k** repeat sales lost	$2.17 million opportunity to convert
>5 seconds	Exceptional SLA, invoked manually when a website is known to be occurring cyber incidents	60+ seconds	Requires admin to manually change policies in security product.	$16 million repeat sales	$49 million opportunity to convert	**>$16k** repeat sales lost	$2.17 million opportunity to convert
>10 seconds	Defined service level agreement using automated mitigation, assuming mixture of known and unknown attacks	10+ seconds	Includes time for redirect to scrubbing centers, analysis and mitigation.	$36 million repeat sales	$49 million opportunity to convert	**>$36k** repeat sales lost	$2.17 million opportunity to convert
>18 seconds	Defined service level agreement using automated mitigation, assuming mixture of known and unknown attacks	18+ seconds	Includes time for redirect to scrubbing centers, analysis and mitigation.	$68 million repeat sales	$49 million opportunity to convert	**>$68k** repeat sales lost	$2.17 million opportunity to convert
A few seconds	Generic statement assuming no defined service level agreement, automation and a mixture of known and unknown attacks	3-60+ seconds	Not a tangible SLA - Includes time for redirect to scrubbing centers, analysis and mitigation.	>$240 million repeat sales	$49 million opportunity to convert	**~$240k+** repeat sales lost	$2.17 million opportunity to convert

Source: [illegible]

Delving into the impact of an extended DDoS incident on individual industries shows us the consequences on our lives, the services we rely on, and how cyber-attackers can severely damage the productivity of our businesses.

Medical

Connected IT systems, medical devices, heating, ventilation, and air conditioning are installed across healthcare networks. When a DDoS attack affects a healthcare provider, click-to-call features, critical care monitors, pharmacy dispensary and other acute employee and patient services can be impacted. If this occurs during a health emergency the implications really can mean the difference between life or death.

> *This was tragically illustrated by a woman in Germany who died during a ransomware attack on the Dusseldorf University Hospital. The hospital couldn't accept emergency patients because of the attack and the woman was sent to a health care facility around 20 miles away.*

Financial

With financial institutions underpinning whole economies they are a prime target for an impactful DDoS attack. A well-executed DDoS attack can interrupt a host of banking services including website access, ATM networks, and online banking platforms, in addition to internal systems and functions that help the bank operate and serve customers, including inter-bank transfers. Beyond the operational impact is the resulting damage to the institution's brand equity and reputation when customers are prohibited from accessing their financial information and funds.

The New Zealand Stock Exchange (NZX) experienced this first-hand when it became the victim of consecutive DDoS attacks. The downtime put millions of dollars at stake. The first attack (volumetric DDoS) resulted in a halt of all trading platforms. NZX managed to mitigate the attack and restore connectivity; however, this was short-lived. The next day NZX found itself shut down again due to the same DDoS attack, and the following day held the same disastrous pattern. This led the NZX Main Board, NZX Debt Market and the Fonterra Shareholders Market to be halted for three days.

Manufacturing

Everything in manufacturing is produced en masse. A revolution in manufacturing systems is underway: substantial recent investment has been directed towards the development of smart manufacturing systems (industrial internet of things (IIoT) that are able to respond in real-time to changes in customer demands, as well as the conditions in the supply chain and in the factory itself. Should the systems ever become compromised it would be incredibly costly and potentially dangerous for just about everyone involved. A well-placed DDoS attack could prevent crucial system changes being made or block the transmission of critical telemetry, design, or production data. Likewise, IoT devices that are hacked can be used to build a variety of botnets to target a totally unrelated organization.

An example of this was the 620Gbps attack against the KrebsOnSecurity website launched almost exclusively by a very large botnet of hacked devices. There are some indications that this attack was launched with the help of a botnet that enslaved a large number of hacked so-called Internet of Things, (IoT) devices — routers, IP cameras and digital video recorders (DVRs) that are exposed to the internet and protected with weak or hard-coded passwords. When the traffic from the attacking system was analyzed it became apparent that it wasn't just from one region of the world or a small subset of networks – it was coming from everywhere.

Telecommunications

Digital-citizens and digital-first businesses are perennially connected to internet services of one form or another. Internet browsing, mobile banking, video-on-demand, social media, music streaming services or live news aggregators; large enterprise organizations and telecoms companies are under pressure like never before to maintain global 24/7 service availability. While individual DDoS-caused attacks can incur one-time costly outages by themselves there is a deeper threat emerging. This threat is related to the recurring impact that incessant DDoS attacks have that harm operations and the quality of service to clients and consumers. Telecoms companies, as internet connectivity and security managed service providers, are therefore under further obligation to protect both their networks and their customers.

Mysterious attackers demonstrated how vulnerable ISPs can be when they managed to bring down the external connections of South Africa's largest ISP, Cool Ideas using DDoS amplification and carpet-bombing attack techniques. As soon as Cool Ideas mitigated the first DDoS attack wave, another hit within minutes which took down the systems once again. Two days later it suffered yet another attack which - unlike the earlier hits – targeted the ISP's website rather than its network.

Energy

This industry continues to strive to deliver alternative energy production, innovations in fossil fuel development, and to become less reliant on the major oil producing nations. It is undergoing a transformative evolution of digitalization for upstream and downstream operations and this has put it squarely in the cross-hairs of cybercriminals. Refineries, pipelines, and waterways are lined with network sensors and internet-connected devices which are vulnerable to cyber-attacks from both domestic and foreign threats. With respect to any nation's critical infrastructure the effects of a well-planned DDoS attack should not be underestimated.

> *This was clearly demonstrated when the electrical grid operations in two huge U.S. population areas — Los Angeles County in California, and Salt Lake County in Utah — were interrupted by a distributed-denial-of-service attack. The attack did not directly disrupt electrical delivery or cause any outages, the Department of Energy confirmed, but caused "interruptions" in "electrical system operations." In this case, "operations" does not refer to electrical delivery to consumers but could cover any computer systems used within the utilities, including those that run office functions or operational software.*

Smart Homes and Offices

Bricks and mortar do not make an office or home smart, it's the devices deployed within that define the level of 'smartness'. The IoT comprises all those assets connected to your Wi-Fi, which aren't computing devices, and deliver efficiencies in areas such as; device management, security, safety automation, heating, ventilation and air conditioning automation, smart ergonomics — the list goes on. But a smart home or office also has its own 'Shadow IT' of devices that all seem innocuous; cup warmers, reading lights, fans, desk humidifiers, plugs and the fridge. Innocuous or not, all of these smart devices are your company's or home's next major security risk. To an IT security professional, the practice of blindly purchasing connected devices is functionally equivalent to finding a USB thumb drive in the parking lot and plugging it in to a system behind the company firewall. The majority of all IoT devices have storage, compute and network connectivity which can be compromised, hijacked, or altered, including being forced into service as part of a distributed denial-of-service (DDoS) attack.

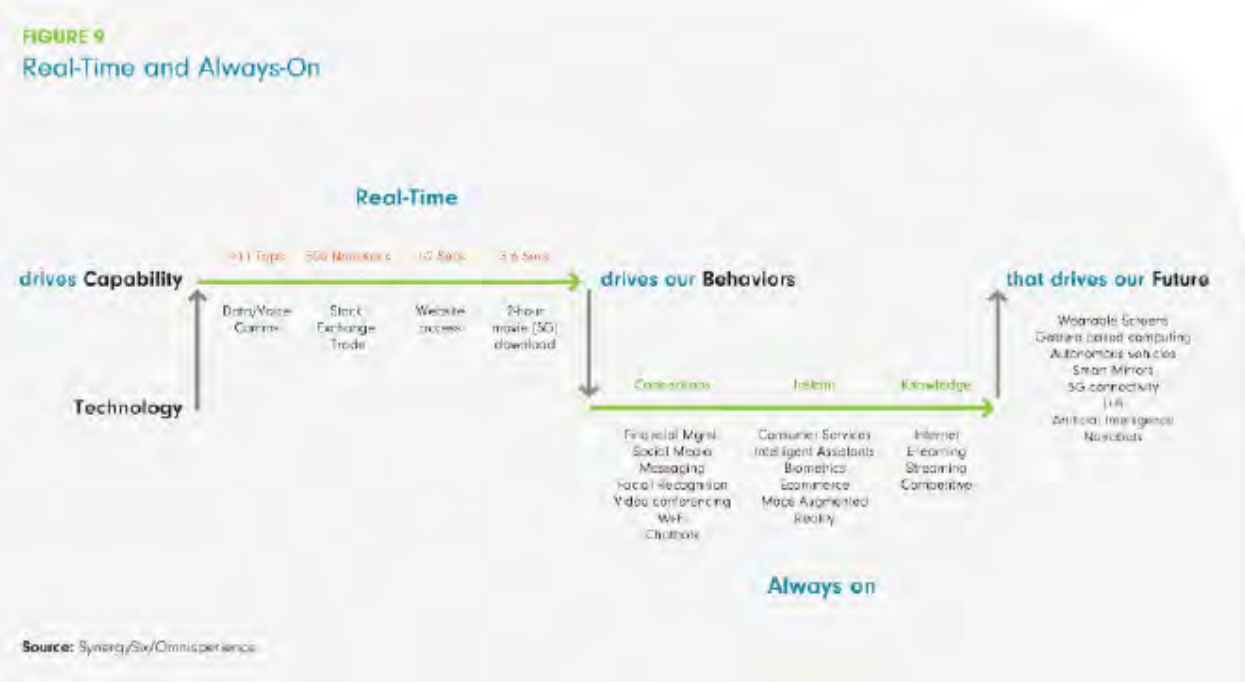
> *A chilling example, of the impact of previously unconnected systems now being openly accessible on the internet, occurred when a targeted DDoS attack was deployed on a building management system of two residential premises in Lappeenranta, Finland. The attack left occupants without heating and hot water, due to the loss of internet connection, at a time when temperatures were way below freezing. The attack lasted three days. The management company (Valtia) explained that an internet connection enables it to monitor and adjust systems remotely (including temperature and ventilation controls) bringing savings in costs and considerably speeds up the company's processes. Where an internet connection isn't enabled "damage will increase, repair time will increase, and costs will rise". The system manufacturer said it was seeing similar attacks around Finland because housing companies or private owners don't want to invest in network security.*

Why We Cannot Tolerate Anything Less Than 'Real-Time' and 'Always-On'

We may not be quite yet zipping around with rockets on our backs, but life in 2020 is still remarkably different than it was even a decade ago. Of course, much of that is due to technology and the internet that touches and enables almost every corner of our lives.

Technology has also made many of us much less patient in more ways than one. With the world at our fingertips, we want to know answers right away. Why wait around for a conclusion when we can find it within a few taps and a swipe? With decreased exposure to waiting for results we may be more inclined than ever to complain, look for alternatives, or change opinions in an instant.

Everything we do in our business and social lives is about speed, convenience and accessibility. Figure 9 provides an example of how technology is delivering a real-time experience that modifies our behaviors when connecting, engaging, and expanding our knowledge. These experiences and behaviors are continually recognized by the industries that entice us to change our attitudes of acceptance, exploiting their research and development to accelerate the adoption of their technologies to modify our acceptance of 'always on' to meet individual needs. It is essential, however, to first protect the technology that is transforming our behaviors and expectations of 'always on in real-time'.



Size Does Matter

You do not need to be the size of Amazon Web Services (which was subjected to a 2.3Tbps DDoS attack in 2020) to be identified as a prime target. You could fit into one of many other categories, such as: 1) an organization that has value in the data assets it retains, ideal for using a diversionary DDoS attack while deploying malware to encrypt, delete, steal, or use that data for ransom purposes or, 2) an outsourcing service provider, where the incapacitation of the network will affect 100s if not 1,000s of clients. Google is a prime example where the recently announced 2.5Tbps DDoS attack on them in 2017 fits into the AWS mold. It's not just the provider that is impacted, think about the hundreds of millions of people and businesses of all sizes that depend on Google's services either for work or for personal use. Fortunately, the company was able to mitigate the attack. Other organizations may not be so well-defended.

The larger (size and duration) DDoS attacks, when deployed, stand out from the norm in the same way as if someone tried to hide their activities when stealing $1,000 from your check- in account. If they withdrew $5 every couple of days, it would take you a longer period to realize what was happening. As a dedicated DDoS mitigation provider, our analysis consistently finds that the overwhelming majority of DDoS attacks are, in fact, short and sub-saturating. To identify and stop these attacks, similar to the stopping the thief on their first attempt to steal your $5, requires a real-time specialist mitigation solution that is able to automatically detect such DDoS attacks among normal traffic and remove them with surgical precision.

This has proven to be a significant challenge for legacy DDoS protection solutions that often fall short when it comes to effectively detecting and mitigating smaller - but increasingly sophisticated - attacks. When the really large attacks do strike, this can be dealt with using a hybrid solution; combining the fast, accurate, on-premises protection with automatic redirection to a cloud scrubbing service which has the capacity to remove the majority of any attack packets which would have caused link saturation.

Thieves will adapt their methods of stealing your money to evade being caught again. Our statistics - taken from customer experiences - indicate that cybercriminals have continued to adjust their attack methods over the past six months by deploying more multi-vector attacks and launching a greater number of larger (10-100s of Gbps) attacks than in the past. More specifically, the key findings were as follows:

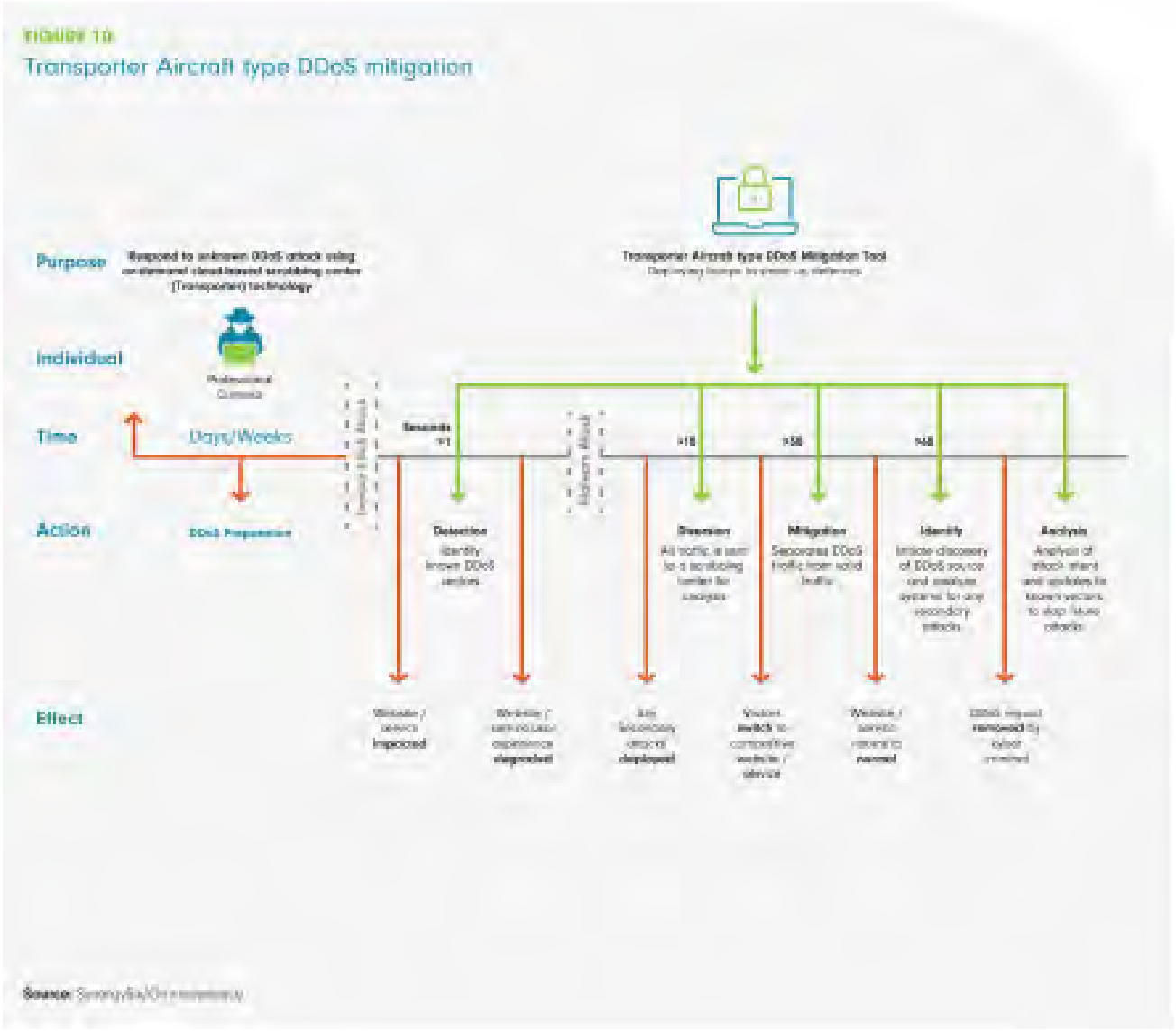
- 95% of attacks were less than 5Gbps
- Larger attacks ranging from 10-100s Gbps increased by 50%
- An increasing use of packet sizes >128 bytes corresponds with the increase in volumetric attacks
- Observed DDoS attacks remain short with around 84% less than 10 minutes in duration
- Multi-vector attacks continue to grow in popularity and the number of vectors used
- The average provider customer is attacked eight times per day. While this is significant it has remained consistent over recent years

Based on these statistics, organizations should recognize that their security tools need to continually adapt to the latest strategies of the cybercriminal. Although most DDoS attacks recorded in the industry continue to be relatively small this does not mean that they don't cause significant disruption. Size does matter.

Time-To-Mitigation: Don't Deploy a Transporter for a Jet Fighter Mission

Popular DDoS protection choices, such as on-demand cloud-based scrubbing, may appear innovative and to offer flexibility (defense in-depth). But these categories of solutions are secondary defense mitigators – similar to a transporter aircraft bringing in troops to shore up defenses while the strategists determine the next push. By the time the strategist has reacted and diverted the enemy (traffic) towards the re-positioned defense forces (cloud scrubbing service) and commenced mitigation, the targeted network has most likely already experienced significant disruption, see Figure 10.

FIGURE 10:
Transporter Aircraft type DDoS mitigation

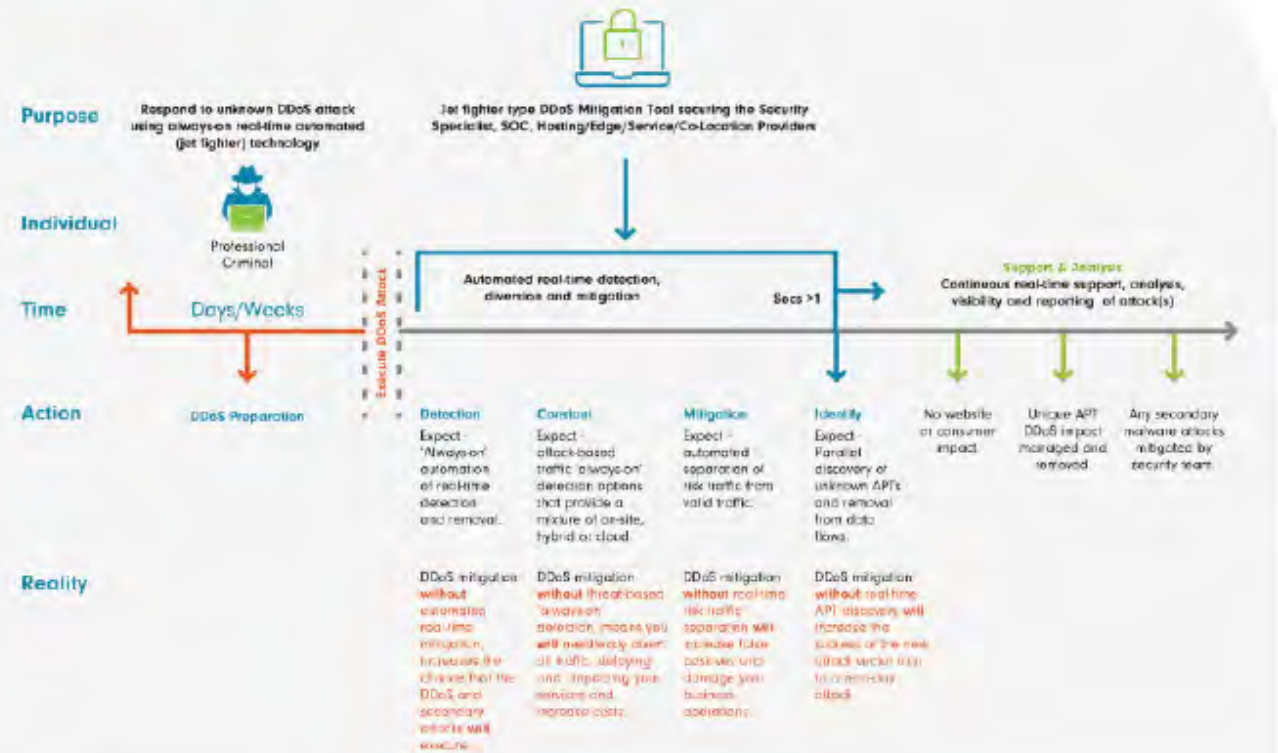


The frequent, short duration attacks that now impact organizations need a rapid reaction force that is always available to respond effectively in real-time. Resembling a jet fighter, Figure 11 shows the need to be decisive and understand that time-to-mitigation (TTM) is critical with today's DDoS threat landscape: detection and mitigation must happen in seconds, not minutes.

As you have no advance knowledge of the type of each incoming DDoS attack it is essential that an automatic system is analyzing traffic during those initial seconds - to minimize TTM and surgically remove the risk - leaving the good data to flow unimpeded. Any delays during the initial seconds, either by the security tools or involvement of security analysts, increases the opportunity for the DDoS and secondary attacks to execute the intent to degrade services and network performance, inhibiting valid traffic from executing on its purpose and opening up the possibility for a zero-day compromise.

FIGURE 11

Jet fighter type DDoS mitigation



Source: SynergySix/Omniperience

What Can You Do Now to Help Secure Your Future and Contribute to a Safer Internet?

When looking for a tool that delivers the most effective DDoS mitigation it is essential to evaluate the capabilities of different vendors and how they can meet your needs. This requirement doesn't change if you are new to DDoS protection or updating an existing mitigation solution. Discussions between yourself and the vendors is critical to determine the true DDoS solution capabilities and avoid wasting your valuable time – and budget.

Any arguments raised when evaluating if the added security levels are a cost of or a cost to a business can be wiped out by the bottom line. To help convey the value of rethinking your DDoS incident defense strategy - and if the tools in place are adequate - you can refer to financial impacts resulting from previously documented attacks. There are also the hidden – but immediate – cost implications as set out in Tables 2 & 3.

DDoS Provider Evaluation Assessment

This evaluation assessment can help you align your experience and understanding of DDoS attacks to the most appropriate DDoS mitigation provider.

	Questions	Context and Response	
1	Existing Provider	Concerns and Needs	
2	Do you have dedicated internal specialists	Network Security	Yes/No – Examples
		Incident Response	Yes/No – Examples
3	Have you experienced a DDoS incident?	Yes/No/Unknown	
4	If 'Yes' to Q3, what type(s) of incidents have you needed to respond to?	Small (<10Gbps)	Yes/No – Examples
		Large (>10Gbps)	Yes/No – Examples
		Short (<10 minutes)	Yes/No – Examples
		Long (>10 minutes)	Yes/No – Examples
5	If 'No' or 'Unknown' to Q3, what type(s) of DDoS incidents do you believe would harm your company the most?	Small (size)	Examples
		Large (size)	Examples
		Short (duration)	Examples
		Long (duration)	Examples
6	What % of DDoS attacks are you experiencing?	Small (size)	% of 100%
		Large (size)	% of 100%
		Short (duration)	% of 100%
		Long (duration)	% of 100%
7	Have you experienced diversionary DDoS attacks, coinciding with other cyber-incidents?	Yes/No/Unknown – any context	
8	If 'no' or 'Unknown', to Q7, would you like to have your network monitored for the presence of DDoS?	Yes/No/Undecided	
9	Do you have a preference where you would run your DDoS mitigation tools?	On-Premise	Yes/No/Undecided
		Cloud	Yes/No/Undecided
		Hybrid (On-Premise + Cloud)	Yes/No/Undecided
		Service Provider	Yes/No/Undecided

DDoS Security Vendor Capability Assessment Sheet

If you are thinking about interviewing a potential new or existing vendor of DDoS security:

	Questions	Context and Response
1	Is the vendor business focused mainly on DDoS mitigation?	Yes/No/Unknown any context
2	Does the vendor have technical support coverage in your region?	Yes/No/Unknown locations and residence of 24 x 7 support
3	Can you engage directly with the vendors engineering and product leaders?	Yes/No/Unknown who, roles and how
4	Does the vendor allow you to evaluate (Proof of Value) the DDoS protection solution to ensure it meets your needs?	Yes/No/Unknown implementation time and duration of PoV
5	Does the vendor allow you to purchase full DDoS mitigation capabilities independent of your network capacity?	Yes/No are there any exceptions?
6	Does the vendor pricing model align to your purchasing requirements?	Yes/No how can you purchase perpetual/subscription (monthly, quarterly, yearly)
7	What are the baseline support services provided with the DDoS solutions?	9 x 5, 12 x 7, 24 x 7. What if any additional costs need to be paid to increase the baseline levels of support?
8	Can you engage with the vendor's reference customers in region/vertical?	Yes/No/Unknown any context/evidence

DDoS Security Vendor Technical Excellence Assessment Sheet

	Questions	Context and Response
1	Can the vendor offer 'real-time' TTM, <1 second, for known and unknown attack types?	Yes/No/Unknown any context/evidence that explains the architecture involved
2	What is the operational time to deploy the vendors 'real-time' offering?	Installation/connections/policies all active
3	Can the vendor offer 'On-Demand' DDoS mitigation?	Yes/No/Unknown any context/evidence
4	What is the operational time to deploy for their 'on-demand' service?	Yes/No/Unknown any context/evidence
5	Can the vendor offer a hybrid DDoS mitigation architecture?	Yes/No/Unknown any context that describes operational architecture
6	Can the vendor offer a managed DDoS service?	Yes/No/Unknown any context that describes operational architecture and responsibilities of alert mitigation
7	Does the managed DDoS provider allow you to update protection policies?	Yes/No/Unknown any context that describes operational management
8	Can the vendor offer manual and automated traffic rerouting to a local scrubbing center?	Yes/No/Unknown any context that describes operational architecture, control of re-routing and responsibilities of alert mitigation
9	What line speed can the vendor support without redirecting to a scrubbing center?	Yes/No/Unknown any context that describes architecture capability and performance
10	Does the vendor provide syslog output for consumption by other security systems, such as an SIEM?	Yes/No/Unknown any context that describes integration with SIEM and other decision analysis tools
11	Does the vendor protect volumetric and state-exhaustion DDoS attacks at Layers 3, 4 and 7 by default?	Yes/No/Unknown any context

DDoS Security Vendor Technical Alliances Assessment Sheet

	Questions	Context and Response
1	How open is the technology to enabling integration with existing systems, including REST APIs for system and policy control?	Yes/No/Unknown any context that describes architecture capability and integration controls
2	What technology relationship does the vendor have with their cloud scrubbing operator?	Context that describes any vendor contractual agreements
3	What is the primary business of the vendor's cloud scrubbing partner?	Cloud /Outsourcing /Security Provider / MSSP / Hosting Provider / Dedicated Scrubbing
4	Do the vendor's managed services providers use their [vendor] DDoS tools for their own operations?	Yes/No/Unknown any context

Contact ZCorum for more information on DDoS solutions:

800-909-9441
info@ZCorum.com

Or, visit our website to learn more.

ZCorum™

ZCorum provides broadband Internet and communication solutions to telcos, cable companies, utilities, and municipalities, assisting in all facets of broadband implementation, integration, engineering and consulting, network monitoring and diagnostics. ZCorum also offers wholesale, private-labeled Internet services, including data and VoIP provisioning, email, Web hosting, and 24x7 support for end-users, enabling service providers to compete effectively in their local rural and suburban markets. ZCorum is headquartered in Alpharetta, GA. For more information, please visit ZCorum.com or contact us at 1-800-909-9441.

corero

For over a decade, Corero has been providing state-of-the-art, highly effective, real-time automatic DDoS protection solutions for enterprise, hosting and service provider customers around the world. Our SmartWall® DDoS mitigation solutions protect on-premise, cloud, virtual and hybrid environments. For more on Corero's diverse deployment models, click here. If you'd like to learn more, please contact us.