www.globalcyberalliance.org

GLOBAL CYBER ALLIANCE™

THE ECONOMIC VALUE OF DNS SECURITY

Adam Shostack, Jay Jacobs and Wade Baker

Introduction

The Domain Name System (DNS) is a critical component of the Internet. It serves as a translator between the human-recognizable domain names and machine-recognizable locations on the Internet and is considered a core service for the functioning of the Internet[1]. While DNS is not commonly used as a security control, it has been used for infrastructure security services. In this paper we investigate a control we are calling protective DNS (also known as a "DNS firewall") — a DNS service that will process a request as normal, but it will prevent the domain translation from occurring for any domains that are deemed to be malicious.

This research quantifies the loss avoidance attributable to DNS firewalls. Not only do we find that DNS firewalls are an effective security control, the availability of open or free DNS firewalls make the solution very cost effective. Moreover, online tutorials and relative ease of configuration makes implementation of this effective security control simple, even for home or personal use.

In summary, DNS firewalls could have mitigated one-third of the incidents we studied and could have prevented $10 billion in losses in those incidents. Furthermore, because it is likely that a protective DNS (PDNS) could have had a role in stopping one-third of all breaches, if the global loss from breaches were $300 billion, for example, a PDNS could play a role in preventing $100 billion in losses.

[1] For example, Sender Policy Framework, Domain Key Identified Mail (DKIM) or DNS-based Authentication of Named Entities (DANE).

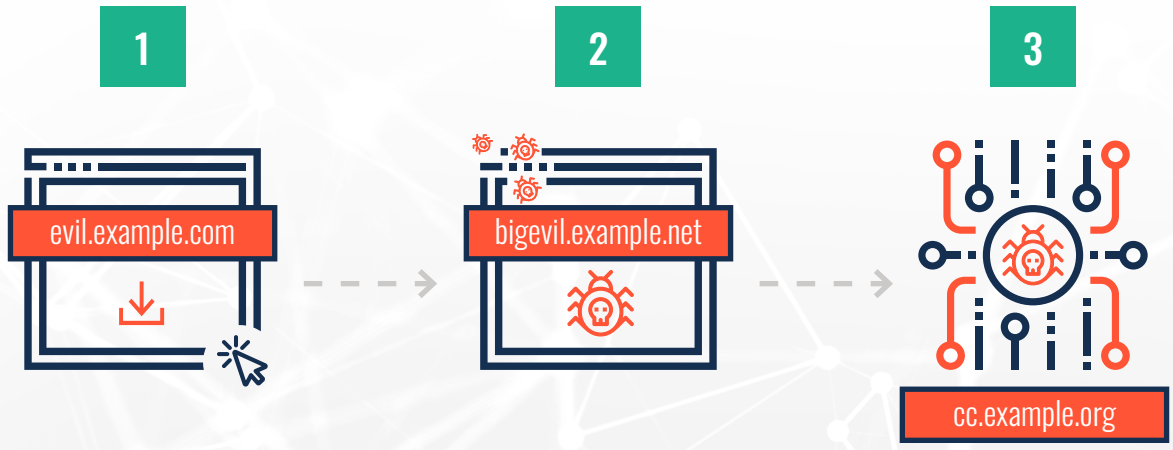
Overview

The Domain Name System (DNS) is fundamental to the operation of the internet. DNS provides translation from human readable names, such as 'globalcyberalliance.org' to computer addresses like 35.202.169.15.

A DNS firewall[2] protects users by automatically blocking access to known malicious and unwanted websites. Let's look at a common scenario then show how it changes with a DNS firewall.

WITHOUT A DNS FIREWALL

1. A user clicks on a link, visits a dangerous website (evil.example.com) and downloads a malware installer.
2. The installer connects to a site (bigevil.example.net) with additional malware that further infects the system.[3]
3. The malware communicates to Command and Control C&C (cc.example.org) (Command and Control) infrastructure which can then exploit the system for malicious purposes



[2] "DNS firewall" is one name for this use of DNS. Other names include "DNS filtering" and "DNS blocking".

[3] The downloader/dropper malware is separate from this second piece of malware so the downloader/dropper owner can then sell access to a ready-to-infect system.

WITH A DNS FIREWALL

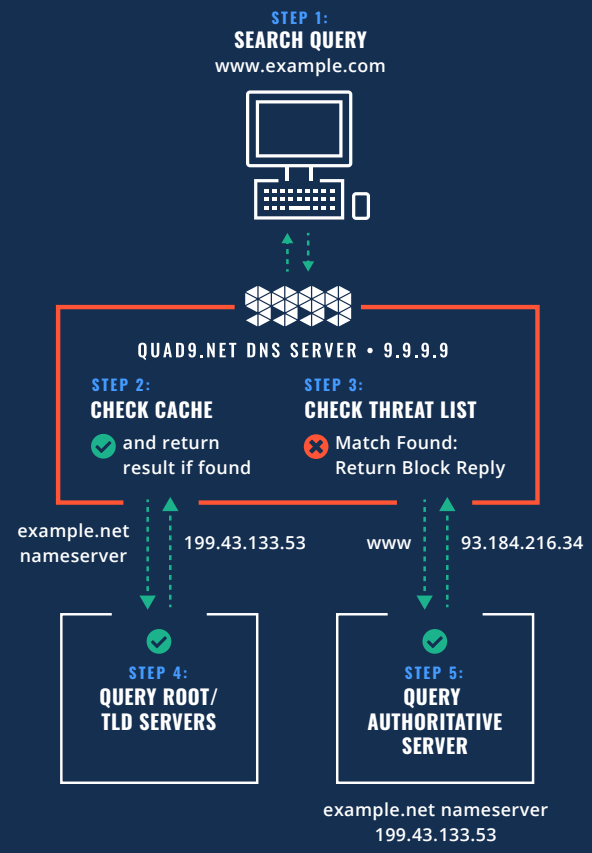
1. When a person clicks on the (malicious) link, their browser contacts a DNS server to resolve the domain.[4] At that step, if the server is aware that the domain is malicious, it can respond with a "not found" message which will cause the browser to issue a "Can't find that site" error. This effectively prevents the initial malware installation.

2. If the initial installer succeeds, malware frequently connects to one or more domains for additional malware. Again, if the DNS is aware a domain is malicious or being misused, it can respond with a "not found" message which again will interrupt the request, preventing the connection and the downloading of the subsequent malware.

3. If the malware does get installed, then it will most likely attempt to communicate to "command and control" infrastructure on a third domain, requiring additional name translation. A DNS firewall can interrupt this communication and prevent the malware from receiving instructions or exfiltrating data.

A DNS firewall is simple to deploy, because it does not require agent software on each host. Rather it replaces a piece of already-used infrastructure. This also makes it relatively inexpensive and an easily-managed central point of control. But how effective is a DNS firewall at preventing incidents? This paper examines the threat landscape and how a DNS firewall can mitigate risk. Specifically, we quantify the loss avoidance attributable to DNS firewalls. We find that DNS firewalls, such as the one offered by Quad9, can have a dramatic effect on rates of attacker success and the impact of that success.

[4] There are cases where this doesn't happen. Some links are to a numeric URL; DNS information may be cached.



Quad9 is a free DNS security service developed in collaboration with GCA, IBM and Packet Clearing House. Quad9 is just one example of free DNS services available.

HOW DNS FIREWALLS WORK

DNS firewalls work like other firewalls, by interrupting the flow of information to malicious network locations. At the DNS level, malicious domains can be blocked, preventing potentially malicious communications. Step 1 begins with the need to translate a domain name to a routable Internet address. This could be instigated by a person surfing the web or an application attempting to reach a network resource, or by malicious software or instructions. Regardless of the source, all requests are sent to the DNS firewall. In step 2, the DNS firewall checks its local cache to determine if the resolution is cached. If it is found, it will return the routable address; if it is not found, the DNS firewall will check the requested domain name against a list of known malicious destinations. If the request matches a malicious destination, the DNS firewall will return a block reply which effectively prevents the source from reaching out to the malicious destination. However, if the domain name is neither cached nor found on the list of malicious destinations, it will participate in the DNS process as usual, requesting the address from the Root or Top-Level Domain (TLD) servers and eventually the DNS server that knows the routable address of the requested domain name.

Identifying Threats Mitigated by a DNS Firewall

The first step in quantifying loss avoidance attributable to DNS firewalls is to identify threats that rely on DNS for a successful attack. These are threats that could potentially be prevented, detected or otherwise mitigated by a DNS firewall. Identifying those threats requires a well-organized framework of threats suitable for that purpose. Numerous cyber threat frameworks or taxonomies have been proposed over the years, but many suffer from various deficiencies that limit or prevent meaningful threat-control associations. Thankfully, there is no need to reinvent the wheel because a public and proven framework exists that meets our requirements - the Vocabulary for Event Recording and Incident Sharing (VERIS)[5].

THE VERIS FRAMEWORK

The VERIS framework undergirds Verizon's long-running and well-respected Data Breach Investigations Report (DBIR). VERIS was created to provide robust schema for describing security incidents in a structured and repeatable manner. It has been tested and refined through 12 years of research spanning hundreds of thousands of incidents. Furthermore, the framework itself was published nearly 10 years ago and is used by organizations and tools around the world to collect, analyze, and share incident data.

Verizon started an open database of publicly-disclosed incidents called the VERIS Community Database (VCDB)[6]. As the name implies, it uses the VERIS framework and is open to contribution and analysis by the security community. These resources allow us to proceed in a straightforward manner. First, we use the VERIS framework to identify threats that could have been prevented with the use of a DNS firewall. Next, we can use our definition to identify incidents within the VCDB that are associated with these threats. Basing our analysis on VERIS[7] and the VCDB obviates the need to sift through thousands of incidents from disparate sources to identify those relevant to the current study.

5 http://veriscommunity.net/

6 https://github.com/vz-risk/VCDB

7 VERIS is not the only threat framework, but the availability of data encoded with it makes it a better choice than Shostack's Broad Street taxonomy, or MITRE's STIX or ATT&CK.

ALIGNING DNS FIREWALLS TO VERIS

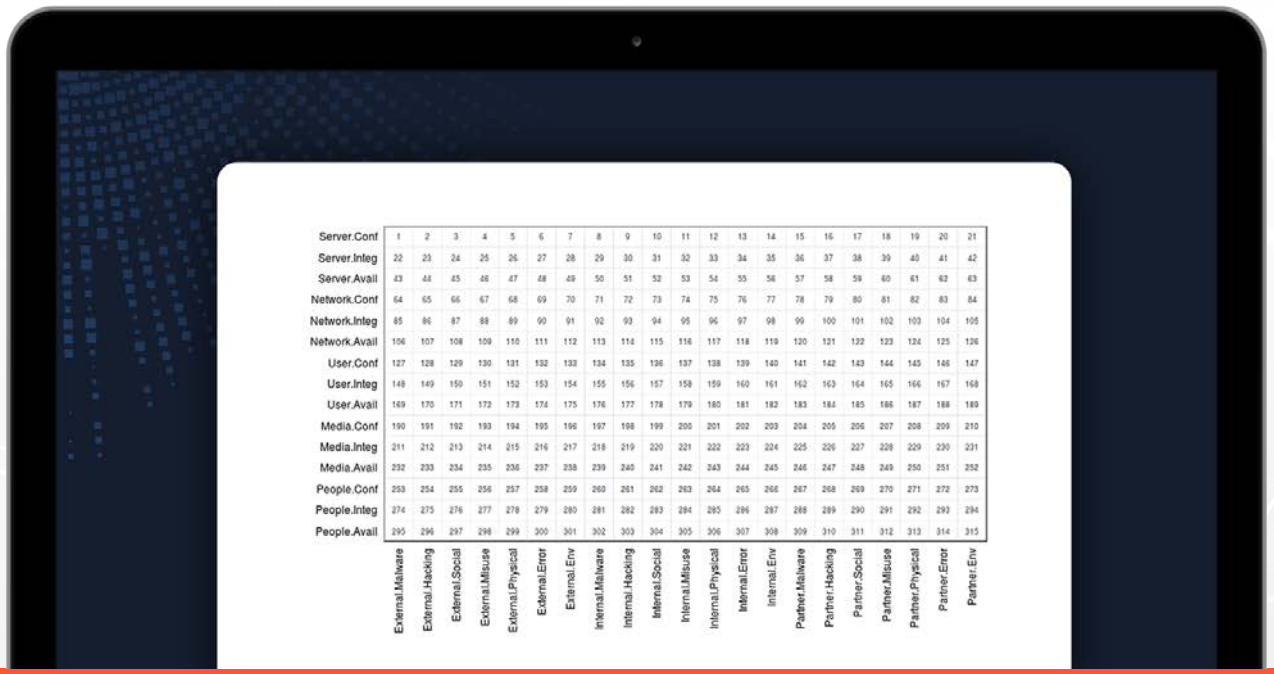
The VERIS framework allows for the collection of threat, incident and response information. This includes data on how quickly the victim organization detects and responds to an incident. In VERIS threats are described using the A4[8] event model. This model translates the narrative of "who did what to what (or whom) with what result?" into a form suitable for sharing and analysis. Thus, classifying a security threat or incident in VERIS essentially means identifying the actors, actions, assets, and attributes (the 4 As) involved. We will focus on the "action" component of VERIS for this effort.

Actions describe what the actor(s) did to cause or contribute to the incident. Every incident has at least one, but most will comprise multiple actions (and often across multiple categories). VERIS specifies seven primary categories of threat actions: malware, hacking, social, misuse, physical, error, and environmental. Each of these high-level categories includes multiple varieties or types of threat actions.

We reviewed all threat actions across the seven categories above to determine those that *might reasonably be mitigated*[9] by a DNS firewall. Appendix A provides a list of selected threat actions and our assessment of the impact of DNS firewalling on those threat actions. The strength of a DNS firewall is not uniform across these threats; it will be directly and highly effective for some, while minimally or indirectly effective for others. Furthermore, a DNS firewall may actively protect against certain threat actions but may only help detect or respond to others. We considered such distinctions during our evaluation, but did not incorporate this into our analysis.

[8] "A4" refers to the four As in the VERIS framework: actor, action, asset and attribute affected.

[9] We will also use the phrase "DNS firewall *is likely relevant* to" to mean the same thing.



Measuring the Frequency of Incidents Relevant to a DNS Firewall

Having identified threats potentially mitigated by a DNS firewall, we are now able to measure the prevalence of associated incidents within VERIS-based datasets. This will provide an estimate of the scope and relevance of DNS firewalls in the landscape of the threats organizations are likely to encounter. Said simply, we seek to answer the question **"What fraction of incidents could be mitigated with the implementation of a DNS firewall?"**

To help us answer that question, we turned to the team at Verizon that produces the annual DBIR. Using VCDB as a testbed, we developed an analysis to tally the number of confirmed data breaches that involved the threat actions identified previously (and listed in Appendix A).

The Verizon team then ran the analysis against their private DBIR dataset and provided us with the results.

The DBIR dataset contains 11,079 confirmed data breaches[10] collected and analyzed over the last five years. Of these breaches, 3,668 involved at least one of the threat actions which would have been potentially mitigated by a DNS firewall. **This means that a DNS firewall is a relevant control against one-third of the breaches in the DBIR dataset over the last five years** (See Figure A)**.**

Figure A: DNS Firewall is a Relevant Control Against One-Third of Reported Breaches

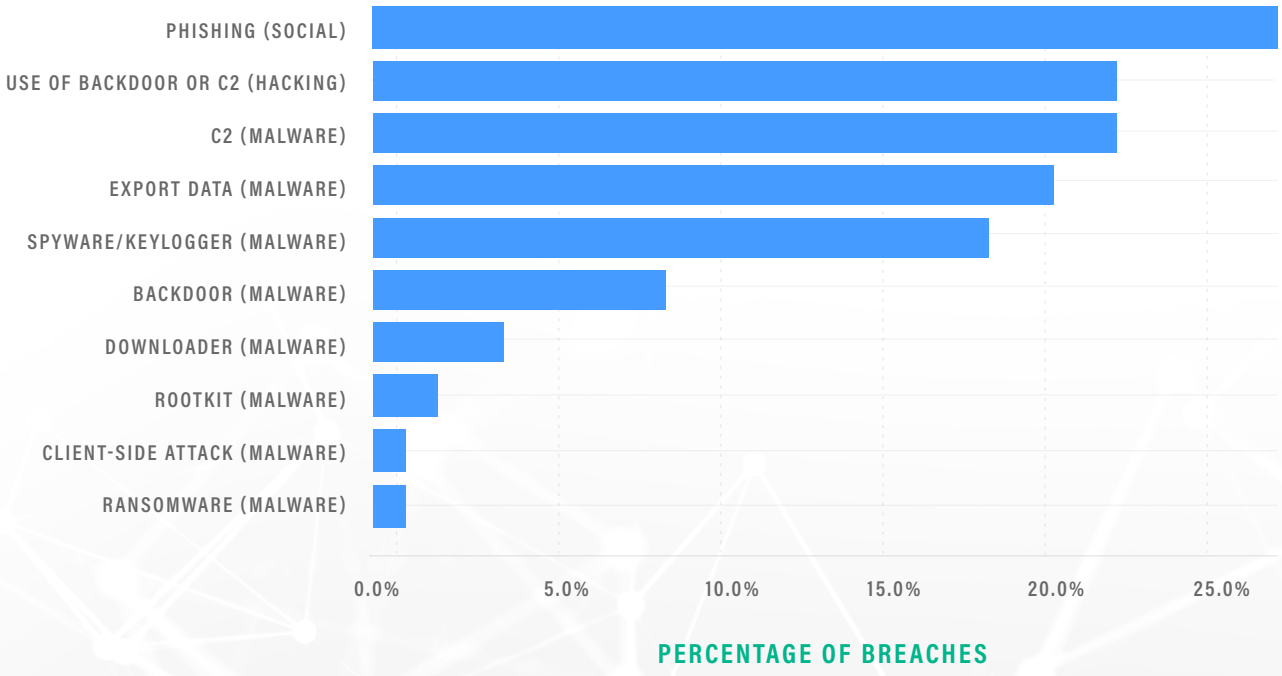
[10] The DBIR makes the following distinction between security incidents and data breaches: An "incident" is a security event that compromises the integrity, confidentiality or availability of an information asset. A "breach" is an incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party (from 2018 DBIR, pg 2). Our analysis is based solely upon the latter.

It should be noted that this estimate is likely at the lower end as the DBIR data only records known threat actions when there are observable indicators of those threat actions.

For example, sometimes it is clear that malware infected a system, but the full range of the malware's functionality could not be determined by Verizon or its partner (for various reasons). Therefore, even if it did have the functionality to communicate with a command and control infrastructure it would not be recorded as such in the data and thus may not have been included among incidents we identified as relevant to a DNS firewall. Because the nature of the data source makes that hard to quantify, we are not measuring every case where a DNS firewall could have protected the victim, and our estimate of the financial impact is probably biased a bit low.

Figure AA adds additional context to this finding. It shows the top VERIS threat actions we identified as relevant to DNS firewalls as well as the percent of breaches tied to each. Keep in mind that these are not mutually exclusive. Most breaches involve multiple threat actions across the chain of events. For this reason, we cannot simply sum the percentages shown to derive the overall proportion. The correct interpretation is that 33% of all breaches in the five-year sample recorded at least one of these threat actions.

Figure AA: Frequency of VERIS threat actions (and category) in Verizon DBIR Data 2012–2017



Organizations and individuals considering Quad9 or another DNS firewall solution can apply that one-third statistic to their threat environment as a ballpark upper end for control relevance.

Estimating Losses

We believe the proportion of breaches in the Verizon dataset potentially mitigated by a DNS firewall (33%) to be the most useful finding to most readers of this report. It is very rare to find a control with the combination of high impact and ease of deployment. We are tempted to just stop the report here. However, losses due to data breaches can vary substantially. So next, we derive an estimate of total losses associated with both the 3,368 breaches identified above and estimates of global losses.

This effort introduces new challenges. Good loss statistics for cybersecurity incidents are difficult to obtain and even harder to aggregate. Using the **Cyentia Library**, a collection of more than 1,300 security industry reports, we were able to find a handful of sources that provide usable data points for our purpose. For this report, we are including all reported costs with an explicit mean or median. Table 1 lists these sources and statistics, and Appendix B provides additional context around these references[11].

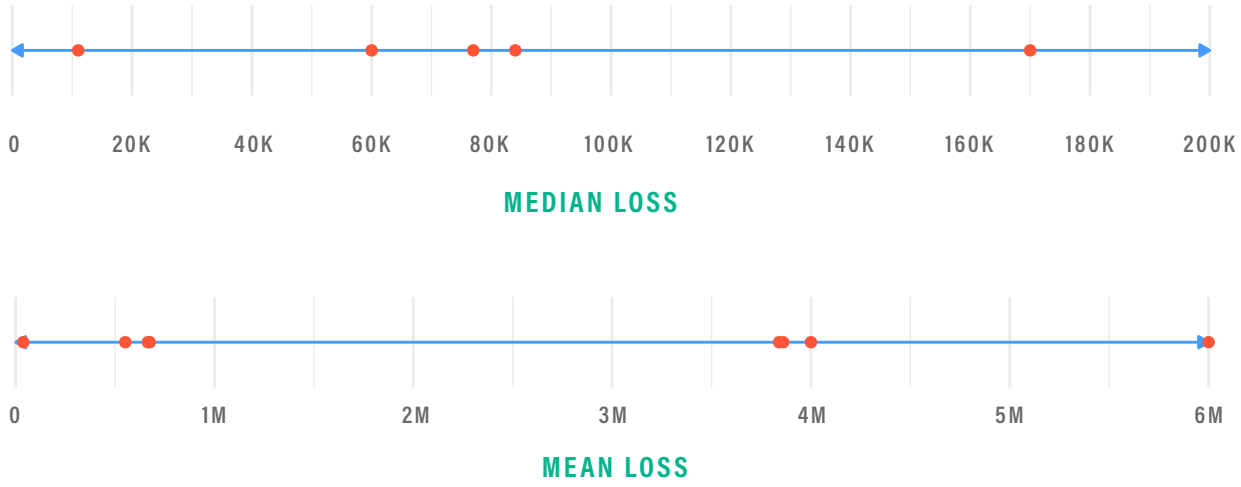
Table 1: Sources and statistics for losses associated with data breaches

YEAR	SOURCE	MEDIAN	MEAN
2015	Kaspersky (Survey) — SMBs	11,000	38,000
2015	Kaspersky (Survey) — Enterprise	84,000	551,000
2015	NetDiligence (Insurance Claims)	76,984	673,767
2016	NetDiligence (Insurance Claims)	60,000	665,000
2016	Romanosky (Advisen)	170,000	6 mil
2017	SailPoint (Survey)		4 mil
2018	Ponemon (Survey)		3.86 mil
2017	Ponemon (Survey)		3.62 mil
2016	Ponemon (Survey)		4 mil

[11] It is worth mentioning that these loss statistics likely overestimate "typical" losses because studies like the ones shown in Table 1 generally focus on memorable, public, or reported breaches. Thus, minor breaches that do not trigger insurance claims or mandatory reporting may not be well represented.

These points are presented visually in Figure B. From both the table above and the chart below, it is easy to see that mean losses are substantially larger than the median across all sources. This indicates a strong right-tail skewing among breach losses. Reported losses typically do not exceed a couple hundred thousand dollars, but a relatively few extremely large losses inflate the mean into the millions. Among the worst publicly reported breaches, that upper tail of losses stretches well into the hundreds of millions.

Figure B: Median and mean values from reports on data breach losses



Despite these wide-ranging statistics and caveats, we can develop a credible loss distribution model that approximates the data shared above. That distribution is captured in Figure C and has a median of $70,000 and a mean of $2.8 million. The top 10% of breaches fall above $3.8 million. The top 5% are above $11 million, and the top 1% exceed $57 million. It even accounts for those rare one-in-a-thousand breaches that exceed $200 million.

> Reported losses typically do not exceed a couple hundred thousand dollars, but a relatively few extremely large losses inflate the mean into the millions.

Figure C: Distribution of per-event losses from a data breach

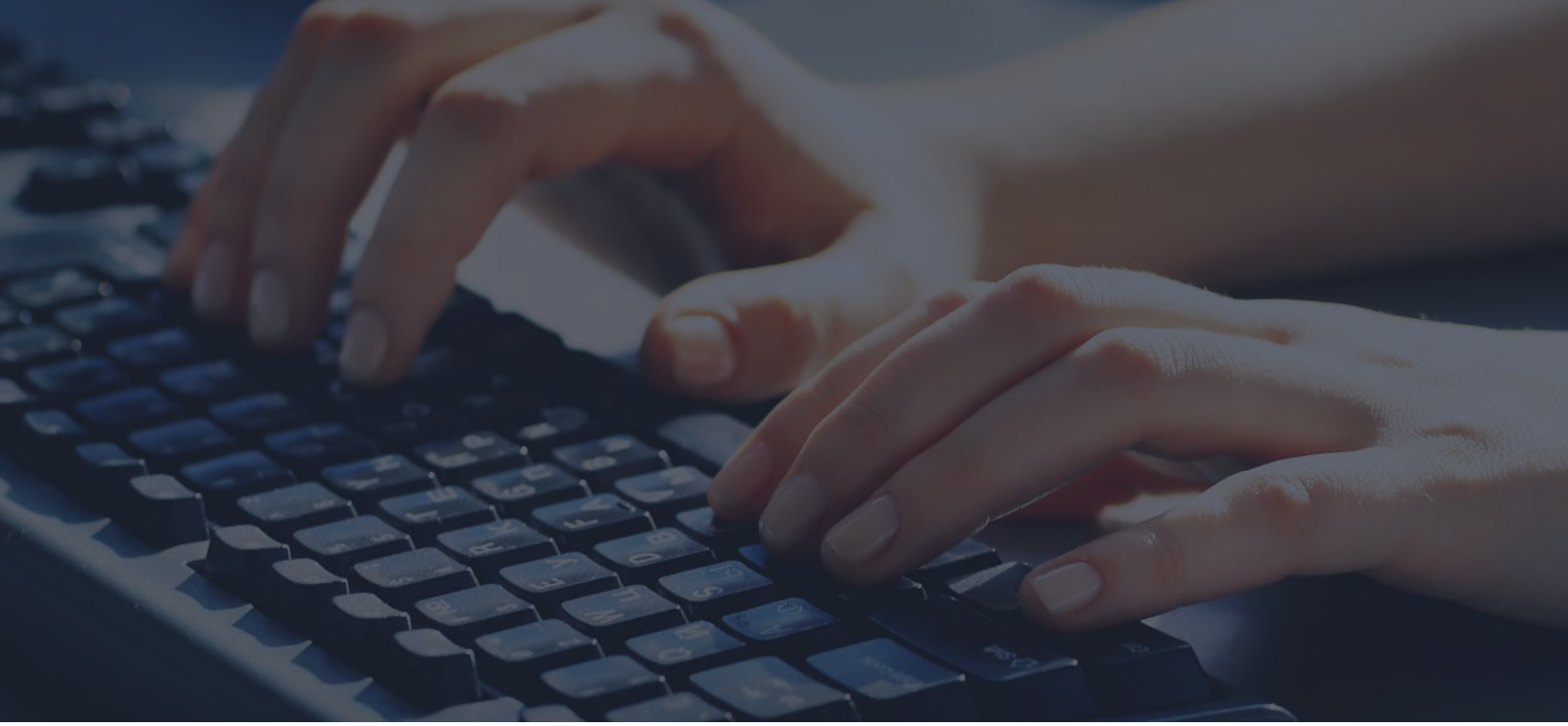
With this distribution of single-event losses in hand, we can simulate losses across the 3,668 breaches identified in the last section from the DBIR dataset. As depicted in Figure D, doing so yields a range of total probable losses of around $8 to $13 billion. **Thus, a DNS firewall solution, such as Quad9, could have played a role in mitigating nearly 3,700 of the 11,079 breaches and approximately $10 billion in losses attributable to those breaches over the last five years.**

Figure D: Total estimated losses across 3,668 breaches identified as relevant to a DNS firewall

The phrase "could have played a role" will likely sound to some as though we are being intentionally vague or backtracking from our findings. We are not. Figure D explicitly displays the uncertainty that exists around the loss statistics. The equivocality of our statement stems less from the estimate of total losses and more from the unknown efficacy of a DNS firewall in mitigating those losses. This is highly dependent upon a range of solution and implementation-specific factors we have no way of measuring. A DNS firewall deployed on a small scope, relying on poor threat intelligence or configured loosely, will make little to no change in probable losses. Indeed, a poorly configured DNS firewall may result in erroneously blocked domains and negative externalities. But a well-designed and deployed solution offers large-scale potential efficacy[12] for relatively little investment[13].

[12] For example, Cisco Umbrella found that 91% of malware leverages DNS for command-control communication.

[13] For example, Quad9 is a free solution that is easy to deploy and leverages solid threat intelligence.



> ...a DNS firewall could prevent between $19 and $37 billion in the U.S. or globally between $150 and $200 billion.

As an additional point of reference, in the spring of 2018, the Council of Economic Advisors released a report estimating that "malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016." [CEC] And McAfee and the Center for Strategic and International Studies estimated in 2018 that global losses from cybercrime are between $445 billion and $600 billion. [MCF] Because our research shows that a DNS Firewall could play a role in preventing one-third of breaches, it is likely it could have played a role in one-third of these losses to the extent that they arise from breaches and not denial-of-service or other non-breach attacks.

For those who feel those numbers are a credible baseline, there is no obvious reason to not extend our analysis that one-third of losses could be prevented, and so, a DNS firewall could prevent between $19 and $37 billion in the U.S. or globally between $150 and $200 billion (again assuming that those losses stemmed from breaches).

Discussion

EXPECTATIONS AND IMPRESSIONS

There are plenty of soundbites which caused reviewers and perhaps even readers to believe, for example, that many of the breaches were due to phishing (an attack which can be impacted by a DNS firewall). For example, a 2018 white paper by Appthority titled "*Enterprise Mobile: The New Threat Vector*" [APP] stated, "A recent study found that 91% of attacks involved spear phishing" and referenced a blog post by Firmex [FRMX] which stated, "91% of attacks between February and September of 2012 involved spear phishing" citing a Trend Micro study from 2012. When we looked at the study from Trend Micro [TREND] titled "*Spear-Phishing Email: Most Favored APT Attack Bait*" we found the study was limited to state-affiliated actors referred to as advanced persistent threat (APT). The study claims they "...analyzed APT-related spear-phishing emails...found, for instance, that 91% of targeted attacks involve spear-phishing emails..." So the original study specifically looked at APT targeted attacks, which is a limited and narrow source of security incidents and should not be used to infer about all breaches or incidents.

This trend continues throughout cyber security research and discussions. Cofense published "*Phishing Response Trends: It's a cluster*" in 2017 [CF]. They open the report by stating, "With 91% of breaches starting with phishing emails, we find ourselves in an arms race against phishing attackers." They cite the source as a Dark Reading article [DR] with a similar quote.

That article references a Phishme (which was purchased by Cofense) publication from 2016 [PHISHME] that makes the claim "91% of cyber attacks and the resulting data breaches begin with a spear phishing email" and cites the same Trend Micro study as above. It is difficult to combat these circular citations that have taken the original research out of context, but by focusing on the Verizon data, we get a much broader set of incidents beyond the limited scope of just APT attacks.

INDIVIDUALS AND USABLE SECURITY

Our dataset is focused on breaches of organizations not on attacks on individuals or families. We are hesitant for two reasons to make recommendations for individuals. First, the attacks they suffer are likely different. Second, it is easy to slide into endless practice lists or blaming of victims, practices we do not support. Nevertheless, we make a strong recommendation for individuals below and discuss the reasons therefor.

Individuals, even early adopters, are likely to have far less technology than even a medium-sized business. As a result, their "attack surface" is both smaller and simpler. The simpler attack surface includes the elimination of categories of issues such as lateral movement, SQL injection, or click fraud. Thus, the issues that remain are more likely to be impacted by a DNS firewall.

When making a list of security advice, it's easy to include the kitchen sink. (Which should be scrubbed regularly with bleach to prevent infection.) Normal people have trouble eating less and exercising more, and jokes about the VCR flashing 12:00 were solved by smarter clocks, not exhortations to fix it. Good advice has to consist of a short list of steps that anyone can easily follow, and the link between advice and how it solves the problem should be easily understood[14].

While we are always cautious about adding another item to the list of things individuals should do to secure themselves, "use a DNS firewall" is important advice for individuals and think that it passes the bar because of its ease of implementation and high impact on a variety of attacks.

Good advice has to consist of a short list of steps that anyone can easily follow, and the link between advice and how it solves the problem should be easily understood[14].

[14] In comparison to https://security.googleblog.com/2015/07/new-research-comparing-how-security.html we collapse 4 distinct authentication recommendations into: "Use a password manager," because a list of 5 items is challenging to remember without mnemonics.

Conclusion

DNS firewall services range from transparent and free, such as Quad9, to commercial services with configurability and logging options. These services are easy to deploy and can have a dramatic effect on rates of attacker success and the impact of that success.

ADVICE

- **Organizations:** A great many organizations are not yet using a DNS firewall. For example, Cisco Umbrella says that 68% of organizations do not. These controls are worth investigating soon for most enterprises.
- **Individuals:** It is worth using a DNS firewall, such as Quad9.
- **Systems manufacturers:** We think systems manufacturers should seriously consider defaulting their systems to use a DNS firewall service or taking other steps to make it easy to turn on.
- **Router makers:** Make it one button to turn on and potentially one click to swap providers.
- **Standards bodies:** DNS firewalls are worthy of consideration in many security standards.

Appendix A: VERIS Threat Actions Potentially Mitigated by a DNS Firewall

For each threat action, we rated our confidence that a DNS firewall might reasonably mitigate this threat action, along a scale of low (L) to high (H).

THREAT CATEGORY	THREAT ACTION	RATING
Social	Phishing	H
Malware	action.malware.variety.C2	H
Malware	action.malware.variety.Downloader	H
Malware	action.malware.variety.Export data	H
Hacking	action.hacking.variety.URL redirector abuse	H
Social	action.social.variety.Baiting	L
Social	action.social.variety.Spam	L
Malware	action.malware.variety.Adware	L
Malware	action.malware.variety.Click fraud	L
Malware	action.malware.variety.Client-side attack	L
Malware	action.malware.variety.Ransomware	L
Malware	action.malware.variety.Rootkit	L
Malware	action.malware.variety.Spyware/Keylogger	L
Malware	action.malware.variety.Worm	L
Hacking	action.hacking.variety.Routing detour	L
Hacking	action.hacking.variety.Use of backdoor or C2	L
Misuse	action.misuse.variety.Illicit content	L
Social	action.social.variety.Scam	M
Malware	action.malware.variety.Backdoor	M
Malware	action.malware.variety.Spam	M
Hacking	action.hacking.variety.RFI	M

Appendix B: Expanded Citations of Sources of Data Breach Loss Statistics

The text we relied on for Table 1 is as follows:

- Kaspersky, **Global IT Risks Survey (2015)**: *"...based on factors like the amount of money spent on reputation re-building and the amount of business lost through terminated contracts or missed opportunities we can estimate that the median cost of a data breach for SMBs is $11,000; and for enterprise organizations the figure is much larger, standing at $84,000. A serious data loss event, on average, costs an SMB around $38,000, while a larger enterprise (>1,500 employees) faces losing a huge $551,000." (5,500 businesses in 2,200 countries)*
- NetDiligance, **Cyber Claims Study (2015)**: *"The median claim was $76,984. The average claim was $673,767." "The average claim for a large company was $4.8 million."*
- NetDiligence, **Cyber Claims Study (2016)**: *"The average breach cost was $665K, down slightly compared to last year's study. The median breach cost was $60K."*
- Romanosky, **Examining the Costs and Causes of Cyber Incidents** (2016): *"Given the heavily skewed cost distribution from these data, use of the statistical mean as a measure of the cost of a data breach (or cyber event) is misleading. As shown in Table 2, while the mean loss for a data breach is almost $6 million, the median loss is only $170k."*
- CyberArk, SailPoint, **The Powers Of Identity Governance And Privileged Access Security** (2017): *"Enterprises surveyed admitted that they lost, on average, over $4 million as a result of a data breach in 2016." (from SailPoint, Market Pulse Survey 2017)*
- Ponemon, **Cost of a Data Breach Study** (2018): *"Average total cost of a data breach: $3.86 million"*
- Ponemon, **Cost of a Data Breach Study** (2017): *"$3.62 million is the average total cost of data breach"*
- Ponemon, **Cost of a Data Breach Study** (2016): *"$4 million is the average total cost of data breach"*

References

[APP] Appthority, “Enterprise Mobile: The New Threat Vector”, 2018, retreived Feb 2019 at http://info.appthority.com/-new-threat-vector-download

[CEC] Council of Economic Advisors, “The Cost of Malicious Cyber Activity to the U.S. Economy”, Feb 2018, retrieved Dec 18th at https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[CF] Cofense, “Phishing Response Trends: It’s a Cluster”, 2017 Retreived Feb 2019 at https://www.cyentia.com/library-item/2017-phishing-response-trends-us-region/

[DBIR] Verizon, “Data Breach Investigations Report” and related (private) data, at https://enterprise.verizon.com/resources/reports/dbir/

[DR] Dark Reading, “91% Of Cyberattacks Start With A Phishing Email”, 2017, retrieved Feb 2019 at https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

[FRMX] Firmex, “Spear Phishing: Who’s Getting Caught?”, retrieved Feb 2019 at https://www.firmex.com/thedealroom/spear-phishing-whos-getting-caught/

[MCF] Lewis, James, McAfee CSIS, “Economic Impact of Cybercrime— No Slowing Down”, Feb 2018, retrieved Dec 18th at https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

[PHISHME] Phihme, “Enterprise Phishing Susceptibility and Resiliency Report”, 2016, retreived at https://cofense.com/enterprise-phishing-susceptibility-report/

[TREND] Trend Micro, “Spear-Phishing Email: Most Favored APT Attack Bait”, retrieved Feb 2019, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

About the Global Cyber Alliance

The Global Cyber Alliance (GCA) is an international, cross-sector effort dedicated to eradicating cyber risk and improving our connected world. We achieve our mission by uniting global communities, implementing concrete solutions, and measuring the effect. GCA, a 501(c)3, was founded in September 2015 by the Manhattan District Attorney's Office, the City of London Police and the Center for Internet Security.

Learn more at **www.globalcyberalliance.org**.