DOMAIN SECURITY

A Critical Component of Enterprise Risk Management

Prepared by

Dave Piscitello, Dr. Colin Strutt, and Lyman Chapin

Interisle Consulting Group, LLC

28 June 2021

Executive Summary

New, evolving, or persistent threats - ransomware, Business Email Compromise, information stealing, and targeted phishing attacks – appear almost daily. Email, counterfeit, or malicious web content are common indicators among such attacks, and they cause financial losses or disruptions to critical services or infrastructures that threaten lives or lifestyles.

Perpetrators of these attacks victimize users through some form of deception; for example, they use domain names or hyperlinks that "look like" high value brands or organizations they have targeted. They also use persuasion (social engineering) to compromise or hijack domain names that can lend temporary legitimacy to their attacks. Cyber-attack perpetrators commonly acquire domain names from registrars that focus on volume and whose business practices in a domain registration marketplace make look-alike domain names easy and cheap to acquire in bulk. The commodity nature of this marketplace leaves little margin or incentive for registrars to implement measures to protect their customer accounts against attack. The combined effect of these factors streamlines the "weaponization" of domain names for criminal or malicious use and exposes risks to enterprises that typically are not addressed proactively.

In this report, we consider *domain security,* which we define as the preventive measures that reduce the risk of harms or losses associated with an organization's domain name portfolio. We explain the threat landscape and the risks these threats pose. We describe incidents in which failing to adopt domain security measures has been the cause of disruption of service, reputational harm, or other losses. We propose what should not be, but apparently *is*, a novel strategy: include domain names in your enterprise risk management. We then explain how to navigate your way to a registrar that can serve as an enterprise risk management partner.

News Cycle Security: A formula for failure

The breadth and depth of the cyber threat landscape is mostly invisible until the report of a successful cyber-attack captures broad public attention. Ransomware attacks on critical infrastructure (*e.g.*, the Colonial Pipeline attack), phishing attacks that exploit the Covid-19 pandemic, denial of service attacks on crypto-exchanges (e.g., EXMO), or a US National Intelligence Council assessment on election tampering by state actors invariably trigger 24-hour news cycles. While such an attack is active, the news cycle focuses on harms, losses, or commercial and social disruption: unsurprisingly, a multi-million dollar extortion payments (again, Colonial Pipeline) or a declaration of international sanctions are hot news. Soon after, however, only "investigative" reporting attempts to identify the source of the attack. Newsworthiness wanes, and cybercrimes recede into the background of public awareness—until the inevitable next attack.

Because incidents and responses attract public attention, there is an overemphasis on attack response and underemphasis on pro-active, preventative measures to detect, identify, and mitigate threats before an attack can occur. This biases decision making and adversely influences enterprise risk management, which is intended to ascribe value to assets, assess threats, estimate the cost to the organization should the assets be lost, and then identify security measures that can prevent threats from being realized through exploitation and attack.

Risk management is a multi-faceted activity. One facet that is absent from a disturbingly large number of organizations spanning nearly every industry and government sector is managing the risk associated with domain assets—specifically, the domain names that organizations register, and that customers and subscribers associate with the organization's online identity and brand.

At Interisle, we see an opportunity for organizations to consider an alternative to news cycle driven security, which is a proven formula for failure: begin by quantifying the losses or harms stemming from attacks that exploit domain names registration services and the Domain Name System directly. Use cyber risk trends analyses prepared by insurers such as Alllianz and Coalition, Inc to complement or serve as an input to your risk management program. We believe that when organizations fold domain names into risk management, they will conclude that adopting domain security - preventive measures to reduce the risk of harms or losses associated with an organization's domain name portfolio – is necessary to ensure a trusted, resilient online identity and presence.

The Cyber Threat Landscape: Direct and Enabling Attacks

Cyber-attacks such as phishing, malware, ransomware, denials of service, and data exfiltration or destruction are *direct* attacks against devices, networks, applications, data repositories, or services. As is the case with legitimate Internet endeavors, the criminals who perpetrate these attacks use domain names or hyperlinks to provide Internet users with a more human-readable way to identify and visit web sites, social networks, and streaming services than numeric Internet addresses. Domain names are an essential resource for operators of spam, malware, or other criminal distribution networks (botnets). Attackers obtain domain names by registering them purposely for their attacks or by stealing them from their rightful owners. Domain registration accounts are frequent targets for attack resource acquisition.

Because cyber investigators actively look for malicious domain registration indicators such as look-alike domains, many attackers prefer to exploit legitimately registered domain names. For example, attackers will attempt to seize control of domain names or domain registration accounts from legitimate holders through a social engineering attack or registration account compromise. In such cases, the domain hijacking is an *enabling attack.* The attacker next uses the hijacked domain in direct attacks against the rightful domain account holder or others.

In a second form of enabling attack, an attacker will exploit a vulnerability to compromise a server and use it as a platform to launch phishing or malware attacks. Gaining administrative privileges of a web hosting server and uploading malicious content is perhaps the most common form of this form of enabling attack. the server compromise, is an *enabling* attack. Table 1 illustrates the ripple effects of DNS hijacking or server compromise attacks.

Direct attacks against domain account holder	Possible consequences to domain holder	Direct attacks against others	Possible consequences to others
Mail redirection	Correspondence or sensitive data disclosure, transaction, or CEO fraud	Domain is used to distribute spam	Spam, malware distribution, phishing, or business email compromise (BEC)
Web server redirection	Disruption of online presence or merchant transactions	Redirection to fake sites, data leak, traffic interception, malicious content hosted	Phishing attack, Malware distribution, credential harvesting
Web site compromise	Reputational harm, Service disruption	Defacement, malicious content insertion, redirection	Loss of confidence in organization
Extortion or domain takeover	Financial loss, online presence disrupted, protracted dispute resolution		Supply chain disruption, necessary service disruption
Data, media, or streaming server redirection	Disruption or critical operations, passive surveillance, data disclosure, alteration, or destruction		Disclosure of personal data or activities

Table 1 Ripple effects of DNS hijacking or server compromise attacks.

For example, Security firm FireEye's analyses of multiple attacks during the January 2019 spate of DNS hijackings confirmed that the attackers used DNS hijacking as the enabling attack.

These incidents occur with disturbing frequency, even among the large enterprises or government services across the globe, as these headlined articles confirm:

28,000 GoDaddy customers breached

MAY 2020 — "GODADDY, THE WORLD'S LARGEST WEB DOMAIN REGISTRAR, HAS SUFFERED FROM A BREACH THAT SAW A BAD ACTOR GAIN LOGIN INFORMATION FOR THE HOSTING ACCOUNTS OF 28,000 CUSTOMERS."

Hackers Control Perl.com Domain Months Before Hijack

MARCH 2021 — "THE PERL.COM DOMAIN WAS HIJACKED IN JANUARY 2021, BUT HACKERS SEEMINGLY TOOK CONTROL OF IT FOUR MONTHS PRIOR, IN SEPTEMBER 2020."

Crooks social-engineered GoDaddy staff

NOVEMBER 2020 — "CROOKS WERE ABLE TO HIJACK TRAFFIC AND EMAIL TO VARIOUS CRYPTOCURRENCY-RELATED WEBSITES AS A RESULT OF A DNS HIJACKING ATTACK ON DOMAINS MANAGED BY GODADDY. THE THREAT ACTORS WERE ABLE TO MODIFY DNS SETTINGS BY TRICKING GODADDY EMPLOYEES INTO HANDING OVER THE CONTROL OF THE TARGETED DOMAINS WITH SOCIAL ENGINEERING ATTACKS"

DNS Hijacking Attacks Target Organizations Worldwide

JANUARY 2019 — "A DNS HIJACKING CAMPAIGN TARGETING ORGANIZATIONS IN VARIOUS SECTORS AROUND THE WORLD MAY BE THE WORK OF THE IRANIAN GOVERNMENT... ACCORDING TO FIREEYE, THE ATTACKERS LEVERAGED DNS HIJACKING FOR THE INITIAL FOOTHOLD INTO THE TARGETED ORGANIZATION'S NETWORK."

"The hackers used three different methods to manipulate DNS records and intercept the victims' traffic. One method involves logging into a DNS provider's administration interface using compromised credentials and changing DNS A records in an effort to intercept email traffic. Another method involves changing DNS NS records after hacking into the victim's domain registrar account… A third DNS hijacking method observed by FireEye in these campaigns involved using a DNS redirector and previously altered A and NS records. In this case, users were redirected to attacker-controlled infrastructure."

Source: Security Week

How serious are threats to domain assets?

In response to the increasing frequency of DNS hijacking attacks, and attacks against government agency web sites, the US Department of Homeland Security (DHS) issued Emergency Directive 19-01, identifying domain name infrastructure tampering as a national information security threat and delegating implementation of the Directive to the Cybersecurity and Security Agency. In the Directive, measures to mitigate enabling attacks like DNS hijacking figure prominently.

These threats are serious, but they are not new.

The DHS Directive includes recommendations from security advisories published by the Anti-Phishing Working Group (APWG), the Canadian Internet Registration Authority (CIRA), and the ICANN Security and Stability Advisory Committee (SSAC). These have been reiterated in CSO, CIO, and domain industry publications like Dark Reading, Forbes, and CIO Digital to encourage domain holders to protect their domain registrations and their DNS infrastructures against exactly the kinds of attacks we see rising again in recent years.

These operational and cybersecurity communities have published many recommendations over the course of 13 years. Among these, the recommendations in Table 2 remain relevant and applicable today, particularly in the context of domain security as a component of enterprise risk management.

Recommended Domain Security measure	Purpose
Protect registrar account credentials from disclosure or misuse.	Use multi-factor authentication for access to domain registration accounts. Apply recommended practices for strong password composition and confidentiality management. Take measures to prevent an attacker who has compromised your domain registration account from altering DNS information to prevent email delivery to your organization, including your domain administrators.
Use registrar locks as a first line of defense against domain abuse.	Registrar or "client" locks reduce the ability of a malicious actor to alter your domain's registration or DNS configuration information, transfer your domain away from you, or instruct the registrar to delete your domain from the DNS.
Use registry locks for additional protections from domain abuse.	Registry locks, especially when combined with registrar transfer lock, harden defenses against unauthorized changes, transfers, or deletions. These locks require human interaction on the part of a registry and the domain holder to validate changes in domain status and further protecting you from a hijacking or other malicious or unauthorized action.
Use DNS Security Extensions, DNSSEC, to establish name resolution legitimacy.	DNSSEC extensions provide cryptographic protection against the unauthorized alteration of DNS information and to enable validation of DNS queries for your domains, to confirm that the web site or other services users visit is the one they intended to visit.
Mitigate human error. - **Routinely audit domain registrations and DNS records**	Routinely audit domain name registrations and DNS. Set reminders to avoid lapses in domain names renewals or configuration error. Compare DNS zone data across primary and secondary name servers against your known, intended DNS configuration to detect unauthorized or unintended changes (human error)
- **Routinely audit domain Whois and billing contact data.**	Compare domain registration and billing contact data for all registrations against your known, intended contacts to detect unauthorized or unintended changes (again, human error).
Employ digital certificate security measures.	Include Certification Authority Authorization resource records (CAA) in your DNS zone data to identify certificate authorities that you authorize to issue digital certificates for your domains. Routinely monitor digital certificates for certificates issued without authorization.
Maintain "provenance" documentation for domain assets.	Keep records of all domain registration transactions, correspondence with registrars or registries, corporate filings, and documents demonstrating copyrights, assigns or intellectual property, to prove your rightful use of your domain names in case of names disputes or should you need to recover a hijacked domain.
Use DMARC, DKIM, and SPF to prove email legitimacy.	Combined, email extensions Domain-based Message Authentication, Reporting, and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) to identify mail servers that you authorize to send spam and to assert content integrity.
Implement defenses to identify and mitigate third-party domain name threats against your brands.	Proactively monitor registration activity and DNS to identify domain names that target your organization's brands directly (e.g., infringement) or indirectly (by incorporating deceptive or similar or look-alike strings in domains that are purposely registered for phishing or other attacks).

Table 2 Recommended Security Measures and Purposes

Domain security adoption is disturbingly low

Recent adoption studies by industry and academia find that domain security adoption is lagging.

Less than three percent (3%) of the domains registered in the COM, NET, and ORG Top-level Domains are DNSSEC-signed (StatDNS May 2021 report). These three TLDs account for over 177 million of approximately 370 million globally registered domain names.

DMARC is configured in only one-third of 5,354 financial industry (bank) domains surveyed in 192 countries (DMARC360, June 2020 report). In a separate, 2019 study by 2500K, **approximately twenty percent (20%) of 25,700 domains surveyed from 10 industry sectors were found to have DMARC policy**, and the adoption across the Fortune 500 barely exceeds this disappointing figure at 23%. These adoption rates become even more troublesome when analyses of deployed DMARC policies revealed that "strict quarantining or rejection of unauthenticated messages remains uncommon", a signal that organizations are not ready to make an all-in commitment to email authentication.

CSC Global's Domain Security Report 2020 studied the domain security measures adopted by the Forbes Global 2000 companies and found more evidence that domain security adoption is low.

> **Seventeen percent (17%) of the Forbes Global 2000 use Registry locks**, the most effective means to prevent domain hijacking.
>
> **Four percent (4%) include certificate authority authorization (CAA) records** in their DNS configurations, an effective way to block unauthorized, malicious digital certificate issuance.
>
> **Three percent (3%) of the Forbes Global 2000 have deployed DNSSEC,** an effective measure to prevent DNS cache poisoning, certain forms of phishing, or redirection attacks.
>
> Source: Domain Security Report 2020

Interisle conducted its own analysis of domain security adoption in the US banking industry. We gathered domain registration and DNS configuration data for all active US banks for which the Federal Deposit Insurance Corporation (FDIC) publishes a web site. Our findings paint an even bleaker picture of domain security adoption.

> **One percent (1%) of the FDIC bank domains use Registry locks**, a worrisome sign that US financials are more seriously exposed to domain hijacking attacks than the Forbes Global 2000.
>
> **Two percent (2%) include certificate authority authorization (CAA) records** in their DNS configurations, and are thus more exposed to malicious certificate threats than the Forbes Global 2000, and
>
> **Thirteen percent (13%) have deployed DNSSEC**, exposing US Financials to DNS cache poisoning, certain forms of phishing, or redirection attacks.
>
> Source: Interisle Consulting Group

When we compare email security measures among these US banks against the findings in the Domain Security 2020 report, we see more exposure to threats (Table 3):

Email security measure	Global Forbes 2000 adoption	FDIC-insured US bank adoption
DMARC	39%	1%
SPF	82%	90%
DKIM	10%	0%

Table 3 Use of in-bailiwick email addresses.

While US banks have adopted Sender Policy Framework, the near zero adoption of the complementary authentication and content security measures provided when DKIM and DMARC are also adopted places these banks at greater risk of email spoofing, phishing, or other email-enabled cyber-attacks than the Forbes 2000.

Limited availability of domain security services

The domain registration marketplace largely consists of retail-focused, *consumer-grade* registration businesses referred to as domain registrars. ICANN's Security and Stability Advisory Committee (SSAC) describes this class of registrar as characteristically volume sales oriented, offering commodity pricing, and often co-marketing complementary services such as web and DNS hosting, email accounts, and secure payment processing, individually or bundled. Conducted in 2009, the SSAC study revealed that "attackers have familiarized themselves with registrar behavior and will exploit certain aspects of automation; for example, knowing that electronic mail is the preferred method of notifying registrants of contact and configuration changes and renewals, attackers often attempt to disrupt delivery to email addresses by modifying DNS configurations." (SSAC) The security incidents that SSAC studied in 2009 are eerily similar to the incidents cited earlier in this paper.

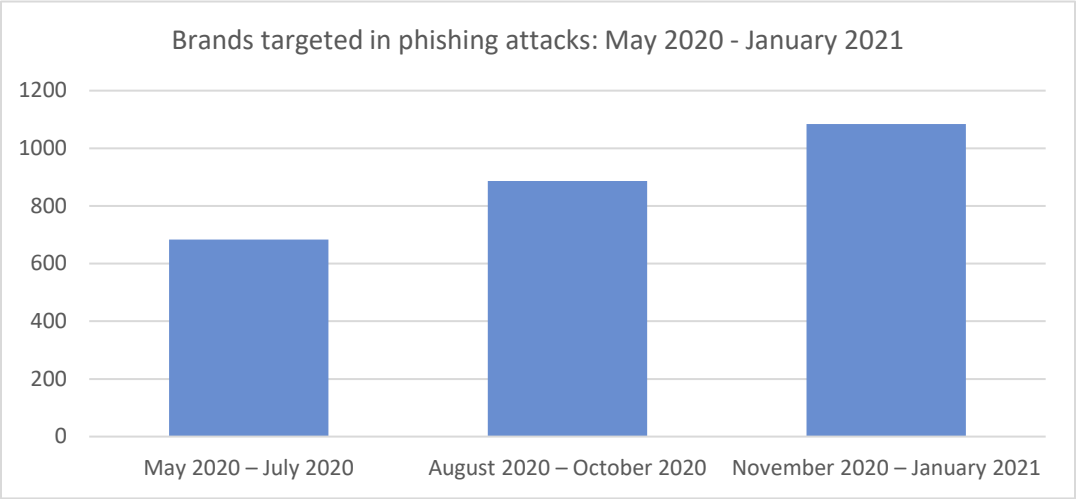
Why so little progress? Race-to-the-bottom pricing models among consumer-grade registrars leaves little margin for them to implement costly security measures. Multi-factor authentication is not widely deployed, and registrar assistance with email authentication and integrity or DNSSEC is rare.

The disappointing rate of adoption for "registry lock" and "registrar lock" services, which require explicit confirmation of changes to registration information, may be due to the confusing and sometimes misrepresented nature of what these locks are. For example, a registrar lock is also called a client lock, which leaves most parties confused over "who is the client?" Similar confusion arises over what actions locks prevent, who acts on the locks themselves (the domain holder, registrar, or registry?) and when locks can be invoked. Investigative reporter Brian Krebs offers the simple explanation that "[w]ith a registry lock in place, your registrar cannot move your domain to another registrar on its own. Doing so requires manual contact verification by the appropriate domain registry" (Krebs). Adoption is also hindered by the fact that many domain registries and registrars still do not offer lock services.

Interisle's study, Criminal Abuse of Domain Names, concluded bulk registration services, name generation tools, anonymous payment methods, and pennies-per domain pricing are indicators of criminality among retail-class registrars that have persistently high concentrations of spam domains under management. The registrars revealed in the Interisle study also appear year after year in the

"most abuse registrars" lists at Spamhaus and in the ICANN-commissioned SIDN Labs report, Statistical Analysis of DNS Abuse in gTLDs.

The study reported that criminals took advantage of "cheap, bulk, auto-generated" services to create and *weaponize* hundreds of exact match or look-alike domains for phishing or other forms of attack. As data from the Cybercrime Information Center shows, brands targeted by phishing using these and other techniques, including names generated pseudo-randomly, have increased significantly since May 2020.



In its 2009 report, SSAC identified an alternative registrar business model that offers "protective measures to meet the needs of customers who place a high value on their domain names, consider their domain names and online presence to be business-critical, or recognize that their business or brands may be highly-targeted for abuse or criminal activities." These measures form a subset of services that Interisle would expect from a registrar that is able to provide domain security that we would characterize as *enterprise-class.* The full suite of an enterprise class registrar services should protect customer domain name registrations against external threats (attackers) as well as internal threats (technical or human errors or failures). It should include services that (i) proactively monitor registration activities of other registrars and DNS activity (name resolution) to identify domain names that target your organization's brands and (ii) can expediently take down the fraudulent domains that criminals can so easily register at consumer-grade registrars.

Only 47% of Forbes 2000 companies use enterprise-class registrars.

Source: Domain Security Report 2020

90% of FDIC-insured US banks use registrars that do not offer adequate services to protect their domain names against hijacking attacks.

Source: Interisle Consulting Group.

A darker statistic emerged when we looked closely at which consumer-grade registrars these US banks use and found that 34% of FDIC-insured banks use registrars that have high concentrations of reported phishing domains at the Cybercrime Information Center.

Include Domain Security in your Enterprise Risk Management

Two important findings emerge from our analysis of risks associated with domain names.

1. **The threat landscape for domain names and their owners is no different from the landscapes for other assets that enterprises fold into enterprise risk management:**

   - Every minute where an online merchant is unable to process transactions is costly.
   - Days, weeks, or months where an organization is held for ransom or mired in dispute resolution over a hijacked domain is both costly and damaging to reputation.
   - Attacks enabled following a domain account hijacking or consequent misuse by an attacker—Business Email Compromise, phishing, ransomware, or data theft/exfiltration—may be costly not only to the targeted organization, but to its customers as well.

2. **Interisle recommends that organizations that cannot afford the loss, misuse, or disruption of their domain assets adopt or amend existing asset management practices to include domain names:**

   1. Identify your domain name portfolio and put all registrations under a common policy and administration.
   2. Ascribe values to your domain assets (tangible and intangible).
   3. List the ways in which each domain asset value may be threatened (e.g., cost or consequence of loss, theft, misuse).
   4. Determine how each threat can be realized: how is each domain name vulnerable to attack or exploitation?
   5. Identify the risk that each threat poses and the means to mitigate each risk.
   6. Identify the likelihood of the threat being realized through attack or exploitation, then prioritize risk against cost of mitigation.

   Registrars that identify as enterprise-class should be able to assist your organization with a domain security needs analysis and recommend services to satisfy these needs.

Domain name asset management is a logical and recommended practice.

"The operational value of a domain name in use—specifically, the assurance that name resolution is highly available and that names in a domain consistently resolve as intended—is of extreme importance to most registrants. Consequently, domain name registrations should be considered as an asset and therefore included in business processes such as asset management, provisioning and risk management programs."

Source: Measures to Protect Registration Services Against Misuse, ICANN SSAC

Domain Security Checklist

Interisle's recommendations for adopting security measures are aligned with industry Best Practices (which in many instances Interisle helped define). ICANN's SSAC compiled a near-exhaustive list of questions to ask registrars its report, A Registrant's Guide to Protecting Domain Name Registration Accounts. These can be summarized into a checklist that closely corresponds to the list of security measures cited earlier in this paper.

Domain security measures: questions for candidate enterprise class registrars
Q: Can you help my organization with a domain asset risk assessment?
A:
Q: Can you help us identify and maintain provenance documentation for our domain names?
A:
Q: What measures do you implement to protect my domain account from compromise or misuse?
A:
Q: What registrar and registry locks do you use to protect my domain account?
A:
Q: Can you help us to incorporate your notification and escalation processes into our domain administration and incident response workflows?
A:
Q: Can you help us implement DNSSEC signing? Key management?
A:
Q: What measures to you adopt to mitigate human error?
A:
Q: What forms of routinely auditing do you provide to ensure that our DNS records registration data, and billing data are accurate, up to date, and protected against disclosure or modification?
A:
Q: Can you help us implement digital certificate security measures?
A:
Q: Can you help us implement email authentication and integrity?
A:
Q: Can you help us implement measures to identify and mitigate third party domain threats against our brands?
A:

The Best Practices Recommendations for Registrars report by the Anti-Phishing Working Group (APWG) makes additional recommendations that registrars can adopt to assist the operational, security, and intellectual property communities with response and mitigation of phishing and other forms of fraud, including evidence preservation for investigative purposes, proactive fraud screening, and phishing domain takedown policies and processes. Ask your candidate enterprise-class registrars how they interact with these communities, as well as with law enforcement and judicial agencies.

Conclusion

The domain security problem space is real and formidable. In this paper, we explain how the domain registration services marketplace is a diverse ecosystem, in which some registrars contribute to the problem while others seek to distinguish themselves by offering domain security services that protect their clients' domain assets. These important assets are compromised via both enabling and direct from indirect and direct attacks by malicious actors or criminals, who are often beneficiaries of the lax security or business practices of other registrars.

We list—and endorse—domain security measures that are widely accepted as recommended practices but remain widely under-adopted. We recommend that organizations include domain names in their enterprise risk management plans and look for enterprise-class registrars to assist them in this critical activity.

Authors

David Piscitello has been involved in Internet technology and security for more than 40 years. Until July 2018, Mr. Piscitello was Vice President for Security and ICT Coordination at ICANN, where he participated in global collaborative efforts by security, operations, and law enforcement communities to mitigate Domain Name System abuse. He also coordinated ICANN's security capacity-building programs and was an invited participant in the Organisation for Economic Co-operation and Development (OECD) Security Expert Group. Dave is an Associate Fellow of the Geneva Centre for Security Policy. He served on the Boards of Directors at the Anti-Phishing Working Group (APWG) and Consumers Against Unsolicited Commercial Email (CAUCE). He is the recipient of M3AAWG's 2019 Mary Litynski Award, which recognizes the lifetime achievements of individuals who have significantly contributed to making the Internet safer. Mr. Piscitello holds a B.A. in Mathematics from Villanova University.

Dr. Colin Strutt has published and spoken extensively on networking technology, name collisions, enterprise management, eBusiness, and scenario planning, and has represented the interests of Digital Equipment, Compaq, and the Financial Services Technology Consortium in national and international industry standards bodies. He holds six patents on enterprise management technology and brings more than forty years of direct experience with information technology, as a developer, architect, and consultant, with recent work including design and operation of a regional public safety network, providing technical expertise relating to patents, and analysis of world-wide Internet use. Dr. Strutt holds a B.A. (with First Class Honours) and Ph.D. in Computer Science from Essex University (UK).

Lyman Chapin has contributed to the development of technologies, standards, and policy for the Internet since 1977, and is widely recognized and respected as a leader in the networking industry and the Internet community. Mr. Chapin is a Life Fellow of the IEEE and has chaired the Internet Architecture Board (IAB), the ACM Special Interest Group on Data Communication (SIGCOMM), and ANSI and ISO Network and Transport layer standards groups. Mr. Chapin was a founding trustee of the Internet Society, and a Director of the Internet Corporation for Assigned Names and Numbers (ICANN). He currently chairs ICANN's Registry Services Technical Evaluation Panel (RSTEP), which is responsible for assessing the impact of new Domain Name System (DNS) registry services on the security and stability of the Internet, and the DNS Stability Panel, which evaluates proposals for new Internationalized Domain Names (IDNs) as country code top-level domains (ccTLDs). He is also a member of ICANN's Security and Stability Advisory Committee (SSAC). He has written many other papers and articles over the past 40 years, including the original specification of the Internet standards process operated by the IETF. Mr. Chapin holds a B.A. in Mathematics from Cornell University.