

The Doorway



A Publication of The Gill Corporation

High-Performance Composite Products Since 1945 • www.thegillcorp.com

Volume 54 • Number 4 • Fall 2018

Cyber Sentinels



5654576 213218 533455


534547657568
675756756756
7867876889
7878678789789
87798797
7867886976
78979878978

2564	5464	6445
54534	464646	4544646
45465	4432113	4313



Cyber Sentinels

We live in a time of unparalleled diversity. Mankind is a melting pot of races, colors and creeds. There are currently 7,106 living languages in the world, including hieroglyphic, sign and 6,500 spoken languages. Regardless of our vast diversity, we have a collective commonality: the emotion of fear.



From early childhood, most people recall being warned against misbehaving and the dangers that lurk beyond the safety of our homes and family. We are taught to follow the rules, be home before dark, avoid unfamiliar places and never talk to strangers. It's telling that generations of people across cultural lines and belief systems have turned the faceless danger into someone real by assigning names to the monster. In the USA, it's the *Bogeyman*. In Germany, Norway, Denmark and The Netherlands he is Butzemann. The Chinese call him *Ou-wu*. Across Latin America he is *El hombre del Saco* and in Russia he is *Baba Yaga*.

As we age, most of us realize the threat is more of a cautionary tale than actual danger, yet the names and warnings persist from one generation to the next. Recently, however, we've come to know a new danger. A very real threat that is strangely reminiscent of Rod Serling's opening soliloquy from the *Twilight Zone*; "*You are traveling through another dimension, a dimension not only of sight and sound but of mind. A journey into a wondrous land whose boundaries are that of imagination.*" Today, the dimension is the Internet and today's "bogeyman" is the modern-day "hacker."

To understand the threat to our cybersecurity requires a bit of a history lesson. The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a *network of*

¹ <https://en.wikipedia.org/wiki/Bogeyman>

networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (www), electronic mail, telephony, and file sharing.

The origins of the Internet date back to research commissioned by the federal government of the United States in the 1960s to build robust, fault-tolerant communication with computer networks in the development of new networking technologies and the merger of many networks. The early 1990s marked the

beginning of the transition to the modern Internet and generated a sustained exponential growth as generations of institutional, personal, and mobile computers were connected to the network. Although the Internet was widely used by academia since the 1980s, commercialization incorporated its services and technologies into virtually every aspect of modern life.

During the late 1990s, it was estimated that traffic on the public Internet grew by 100% per year, while the mean annual growth in the number of Internet users was thought to be between 20% and 50%. As of March 31, 2011 the estimated total number of Internet users was 2.095 billion (30.2% of world population).



In 1993, it is estimated that the Internet carried only 1% of the information flowing through two-way telecommunication. By 2000, this figure had grown to 51%, and by 2007, more than 97% of all telecommunicated information was carried over the Internet.

Clearly, the numbers speak for themselves. As a species, we have become completely dependent on the Internet and the boundless access it allows. Traditional means of communication, education, commerce, and virtually every way we interact now involves the World Wide Web. For private individuals, financial, commercial, educational, state and local governments, the idea you can lock your doors and be safe no longer exists. Cyber-criminals have become increasingly creative in their

efforts to breach our privacy and destroy our sense of security by accessing our records, finances and personal data.

Retailers and banking institutions now spend millions annually to protect their customers from fraud. Companies that once considered IT a necessary but *non-essential* department now view the IT function as an integral part of their businesses. At The Gill Corporation, we deploy a pre-emptive approach to the digital threat and have crafted a plan to protect our internal resources and customers alike.

At the core of our plan is a team of in-house tech experts who work tirelessly to protect our digital infrastructure and keep our electronic devices humming when something goes wrong.

The information technology (IT) function at The Gill Corporation is unique as it answers to so many different “customers.” It supports co-workers, global corporate customers, distribution partners, suppliers, academic institutions, governmental agencies and local community representatives.

To ensure the department is operating at optimal levels, a series of performance metrics are applied to all activities. These metrics measure, monitor, and support the uptime of the environment. (Uptime is the amount of time the systems are online and available to support the business.) For an IT environment to work effectively over a long period of time (or uptime), IT needs to have some regularly planned downtime for maintenance, patching, and upgrades.

On the flip side, a well-functioning IT environment should not have much (if any) “unplanned” downtime. It’s a high-wire act performed on a monitor with a keyboard and mouse.

Maintaining balance in a digital environment requires that the broad array of “customers” have constant access to in-house IT experts. The IT staff need to accommodate and address needs that range from simple (resetting forgotten passwords) to complex (implement, test, adjust and configure new software and hardware). It’s crucial that we have a method to address those needs on a timely basis and that the requests are prioritized correctly based on impact to business. To achieve this, the IT department created the HelpDesk.

The HelpDesk is a central point of contact accessed by email or phone virtually 24/7. Requests for tech support are evaluated to determine scope of work, priority and available resources. The HelpDesk then assigns an IT specialist to resolve the issue and communicates regular progress updates until the issue is resolved.

HelpDesk effectiveness is constantly monitored through a series of metrics that measure success on every interaction they perform. These include:

- Number of calls per week
- Number of calls resolved without any escalation
- Average wait time of a call to be answered
- Number of calls before someone answers
- Time it takes for a call to be resolved

While the HelpDesk is coordinating the day-to-day tech support for the corporation's 1,000 plus employees, the IT department is also responsible for protecting the corporate networks, systems and financial records from cyber-attacks. This requires a pro-active approach to ensure we are vigilant without becoming paranoid, so this part of the plan is constantly evolving to match the burgeoning risks posed by the cyber-criminal community. To manage electronic risks, the IT department constantly:

- Identifies, measures, and manages the business risk related to confidentiality
- Advises and educates the company's management team and employees in regards to the risk in the environment and what is possibly out there
- Advises and educates the company with the correct information so a well-informed decision can be made about risk and possible risk to the environment



- Conducts risk assessments to identify security weaknesses
- Creates a framework of security with various security methods and tools to protect the work environment and the data that are contained within.

Examples of framework security:

- Firewalls
- Anti-viruses
- Various forms of encryption for endpoint
- Security patches
- Identifies, measures, and manages risk related to endpoint, which is classified as:
 - PCs
 - Laptops
 - Smartphones
 - Tablets
 - Terminals
 - End-users
 - Cloud-based storage
 - Emails

- Establishes management processes for any third-party vendors to ensure there is an appropriate degree of security for data
- Maintains compliance by regulatory committees, both private and federal

IT has a plan to support our *internal* needs while our IT specialists work concurrently to monitor outside cyber-threats.

No matter how careful we are, even the savviest individual can be fooled. Many cyber-criminals gain access by tricking unsuspecting individuals to “invite” them into their network, so a core component of the IT protocol is education.

The IT staff routinely conducts trainings, circulates warnings and interacts closely with the workforce to make sure everyone knows what’s out there. In the digital age, you just can’t be too careful.



PHONE SCAMS

ANGER

A caller pretends to be in a position of authority and uses anger to intimidate you.

DONATIONS

A person pretends to be from an organization you might be interested in (political, school, disaster relief group, etc.).

PANIC

When someone calls you pretending to be support and provides a frantic scenario that compromises your safety (like resetting your password or allowing remote access).

VISHING

A pre-recorded message attempts to scam the user into surrendering private information to be used for identity theft.

DIGITAL SCAMS

FRIENDLY EMAILS

An email from a hacked friend's account or one that creates a similar account using your friend's name, but could contain an attachment with malware.

PHISHING

An email purporting to be from a reputable company that induces individuals to reveal personal information, such as passwords and credit card numbers.

77%
of attacks are phishing

PRETEXTING

An email scam where the liar pretends to need information in order to confirm the identity of the person he is talking to.

REVERSE ENGINEERING

A minor attack is executed on your company to expose a vulnerability, and then you are contacted with an offer to "fix" the problem.

SOCIAL MEDIA PHISHING

Someone builds a social media page that mimics a trusted brand with apparent relevant content that persuades you to click and download a malicious file.

TYPO SQUATTING

Use of common typos for brand domains that mimic the brand to gain trust, then collects form information when the typo is not noticed.

EMAIL SCAMS

FROM

Can't recognize the sender's email address.
Email from someone outside one's contacts.
Unusual or out-of-character email sent from a customer, vendor, or partner.
Sender's address has a suspicious domain (like microsoft-support.com).
Sender not known and/or not vouched for by someone trusted.
No business relationship or any past email from sender.
Unexpected or unusual email with an embedded hyperlink or attachment.

TO

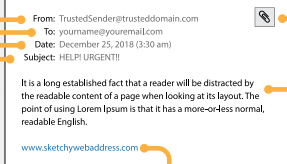
CC'd on an email sent to one or more people not known to you.
Receipt of an email sent to an unusual mix of people, to a random group of people with last names that start with the same letter, or a list of unrelated addresses.

DATE

Receipt of an email at an unusual time that would normally arrive during regular business hours.

SUBJECT

The message is a reply to something never sent or requested.
Receipt of an email with an irrelevant subject line or which doesn't match the message content.



HYPERLINKS

An email received that has long hyperlinks with the rest of the email blank.
A hyperlink displayed in the email message but the link-to address is for a different website.
Hyperlink with a misspelling of a known site, such as AmericanExpress.com where the "m" is two characters: "i" and "n."

CONTENT

The sender is requesting to click on a link or open an attachment to avoid a negative consequence or gain something of value.
The email is out of the ordinary, or has bad grammar or spelling errors.
A request to click a link or open an attachment that seems odd or illogical.
A message that makes one uncomfortable about the sender's request to open an attachment or click a link.
An email asking to view a compromising or embarrassing picture of oneself or someone known to one.

ATTACHMENT

An email attachment that was not expected or that makes no sense in relation to the email message, or not usual from this sender.
Attachment with a possibly dangerous file type.
The only file type that is safe to click on is a .txt file.

The expansion of cyber-crimes has morphed into a worldwide epidemic, affecting almost every country on the globe. This facilitated the formation of cyber-security units which are now permanent fixtures in governments around the globe; for example, the Cyber Division (created in 2002) of the U.S. Federal Bureau of Investigation (FBI).

This unit has 56 field offices staffed with agents and analysts who are formed into cyber-action teams that travel globally to help in computer intrusion cases and gather information that helps to identify cyber-crimes. According to the latest report released by the FBI Internet Crime Complaint Center (IC3), "Victim Losses Exceeded \$1.4 Billion in 2017."²

The numbers are staggering, and recent headlines remind us that hundreds of organizations (Adobe, Anthem, EBay, Equifax, Home Depot, JP Morgan Chase, Marriott, Sony, Target, Yahoo) have been "hacked," jeopardizing sensitive data for both the firm and their customers. These are well-regarded organizations yet they fell victim to digital scams, so recognizing cyber-scams may be our best defense.

Protecting ourselves from cyber-attacks is a daunting task and one we must all embrace. Fortunately, The Gill Corporation relies on a team of dedicated IT specialists with a clear plan of action to thwart the dangers that lurk in cyber-space.

² www.fbi.gov/news/stories/2017-internet-crime-report-released-050718

**Our Chairman and
CEO, Stephen Gill,
the shareholders, and
everyone from the top
on down is committed
to maintain our
privacy, do whatever
it takes to protect
both ourselves and
our customers data
and to keep those
monsters in
cyber-space at bay.**



THE GILL CORPORATION

4056 Easy Street, El Monte, California 91731
phone: 626 443-4022 fax: 626 350-5880
email: info@thegillcorp.com

The Gill Corporation – Maryland

Lakeside Business Park
1502 Quarry Drive
Edgewood, Maryland 21040 USA
phone: 410 676-7100 | fax: 410 676-7050
email: sales@thegillcorp.com

*The Gill Corporation – Maryland does not sell
sandwich panels. Contact The Gill Corporation – El Monte
for these products.*

The Gill Corporation – France

Route de l'Aviation
7, allée Etchecopar
64600 Anglet France
phone/téléphone: +33 (0) 5 59 41 25 25
fax/télécopie: +33 (0) 5 59 41 25 00
email: sales@thegillcorp.com

The Gill Corporation Europe, Ltd.

23 Enterprise Road, Balloo Industrial Estate South
Bangor, County Down
BT19 7TA, N. Ireland
phone: +44 (0) 2891 470073
fax: +44 (0) 2891 478247
email: sales@thegillcorp.com

www.thegillcorp.com

© 2019 The Gill Corporation. All Rights Reserved. The Gill Corporation, The Gill Corporation logo, Gillfab composite, Gillcore, HUSHGRID, GillVANA, Gilliner, Gillite, PAA-CORE, and The Doorway are trademarks of The Gill Corporation. The Gill Corporation "Honeycomb Bee" character is a trademark character of The Gill Corporation. Nomex, Korex, Tedlar, and Kevlar are trademarks of Dupont.



THE DOORWAY IS PRINTED ON 10% POST-CONSUMER RECYCLED PAPER
AND SHOULD BE RECYCLED

THE FUNNY SIDE

FUNNIES

Ever wonder about those people who spend \$5.00 each on those little bottles of Evian water?
Try spelling Evian backwards: NAIVE

Why do croutons come in airtight packages?
Aren't they just stale bread to begin with?

If a pig loses its voice, is it disgruntled?

If lawyers are disbarred and clergymen defrocked, doesn't it follow that electricians can be delighted, musicians denoted, cowboys deranged, models deposed, tree surgeons debarked, and dry cleaners depressed?

If FedEx and U.P.S. were to merge, would they call it Fed UP?

Do Lipton Tea employees take coffee breaks?

You never really learn to swear until you learn to drive.

Whatever happened to Preparations A through G?

MONSTER JOKES

Why won't anyone kiss Dracula?
He has bat breath!

Why is it safe to tell a mummy your secret?
It'll keep it under wraps!

What did Frankenstein say to his sweetheart?
"It was love at first fright!"

What should you do if a werewolf climbs in your window?
Run out the door!

What kind of monster loves to disco?
The boogiemani!

Where does a baby ghost go while its parents are at work?
Dayscare!

How do you get to the monster's house?
Walk down the street, then turn right at the dead end!

What kind of dog does Dracula have?
A bloodhound!

