

## Enumerating and Reducing the Threat of Transnational Cyber Extortion against Small and Medium Size Organizations

Gregory M. Bednarski

[gbednars@andrew.cmu.edu](mailto:gbednars@andrew.cmu.edu)

2004 InformationWeek Research Fellowship  
Master of Science Information Security Policy and Management  
The H. John Heinz III School of Public Policy and Management  
Carnegie Mellon University  
September, 2004

*Copyright by Gregory M. Bednarski © 2004. All Rights Reserved*

### ABSTRACT

Cyber extortion is a sophisticated threat, combining computer intrusion, theft, destruction, and modification of data, social engineering, and fear instilled in victims by threats from would-be extortionists. Without a clear understanding of this emerging crime, businesses cannot adequately defend themselves against it. Unfortunately, current existing research documents or statistics on this subject are in short supply, or non-existent. This paper examines cyber extortion not only as an old crime employing new methods, but as a fundamentally changed threat against small and medium sized organizations that rely on information systems in the conduct of their business. An information system actually becomes the object, the liability through which this type of crime is manifested against a target.

Going beyond the specific methods extortionists typically use, the study has reviewed the current understanding of cyber extortion as a crime in itself. To gain understanding of this threat from an organization's perspective, the study presents results of a survey conducted by the author. In contrast to the *perception* they are at low risk to cyber extortion, many organizations actually lack the necessary information security policies and principles to ensure they *actually* are in a low risk category. Finally, the study develops a number of "best practices" intended to help organizations protect themselves against this crime, and dispels a number of myths surrounding the involvement of law enforcement

in an extortion attempt, and the perception of cyber extortion and its defenses. The guidelines and conclusions are derived from careful review of the survey participants' responses regarding actual experience with extortion, as well as an evaluation of some steps they may have taken to prevent cyber extortion in general.

### CHAPTER I: Introduction

A typical Monday, you spend most of the morning catching up on industry reports, scheduling meetings, and reading e-mail. After answering or filing your important messages, you come across a note titled "Customer Information", but from an unfamiliar sender. You open the message only to find a listing of your largest customers' accounts, credit, order histories, and forecasts. A few of your customers compete with each other, but use some of your goods as components in their products. Distribution of this outside the company is strictly forbidden, yet this unknown individual clearly possess the data. Attached to the information is a simple threat: give us cash, or this information goes public. \$27,000 divided equally and deposited into three separate foreign accounts, all in a country with tenuous relations with your government, before the week's end. What do you do?

This is disastrous. If this information leaks, the media will roast your company for allowing confidential information into the hands of competitors. Your customers could take legal action for financial losses, since their sales

forecasts are now public knowledge. Suppliers and potential customers may move to other firms, fearing their sensitive information may not be safe while tied to your electronic ordering systems. You have only questions: who did this? Is this an inside job? Can our IT department fix this hole? Do they even know what's happened? Can our legal counsel shield us from this? Is our lawyer even competent in this area? Do we risk calling the police, or should we just pay the relatively small sum they're asking? What police would we call? Perhaps you could ignore the threat, and hope it goes away? Why haven't we planned for something like this? Where's our policy or standard operating procedures to help us?

Unfortunately, you don't have time to answer those questions right now. The company's president, your boss, has just called you. He's received a disturbing e-mail he'd like you to see...

### **Statement of the Problem**

The increasing reliance of business on internet-based e-commerce provides enormous opportunities and new forms for extortion. While some threats may fail, payoffs are certainly made to some extortionists. It seems likely, therefore, that larger and potentially more dangerous operations should be anticipated. [1] Despite the increased publicity and corporate awareness of security threats, little mention is made of efforts to thwart extortion threats made against individuals and businesses. At least 50% of the companies responding in the 2003 CSI/FBI survey admitted they did not report security breaches to authorities, with 70% of overall respondents fearing the impacts of negative publicity. Although this statistic references cyber crime in general, we can easily apply it to extortion, which includes threats of further damage, and can understand why many organizations wouldn't report this particular crime. From an international perspective, only 44% of responding British companies involved law enforcement after an incident occurred. [2] Consequentially, we find that extortion statistics and published anti-extortion methods at the time of this publication *simply do not exist*. Without meaningful statistics we, as security professionals, would have a difficult time understanding or combating this crime.

### **Purpose of the Study**

The purpose of this research is twofold. First, to generate statistical data via a survey to collect information regarding:

- General demographic data of participants.
- Organizational policy and technical security measures perceived to protect against cyber extortion; Perceptions on cyber extortion exposure.
- Experience with cyber extortion and actions taken in a hypothetical cyber extortion attempt; Perceived damage potential of extortionists' methods.

Second, with the survey data in-hand, to produce a list of guidelines organizations may use to better protect themselves against extortion. These guidelines include policy and technological measures, as well as methods of working with law enforcement.

### **Assumptions of the Study**

All study participants are assumed qualified to answer the questions set forth in the survey questionnaire. Great care was taken to distribute the survey via industry associations catering to upper-tier management in organizations employing significant use of information systems. In the case of direct invitations to study participation, only chief officers of information, security, executive office, and legal matters were included.

Additionally, this paper is written assuming the intended audience is familiar with basic information security concepts.

### **Limitations of the Study**

The study, including all background research, interviews, and survey, was limited to the time between June, 2004 and September, 2004. Organizations could not be compelled to participate, and notice of the survey could only be distributed via cost-free methods (e.g. – no paid newspaper advertisements, no direct mailings).

The transnational perspective of this research levies an additional limitation on the author: language barriers. Examples of cyber extortion in the international press typically point to sources in Eastern Europe, namely Russia.

While a review of the Russian Federation's criminal and law enforcement records may yield useful data in furtherance of this study, the fact the material is written in the Russian language poses a significant barrier for this particular paper.

The survey portion was limited to organizations with less than approximately 10,000 full-time employees. Larger organizations may have more legal, financial, or political powers at their disposal to prevent and respond to this crime, making smaller organizations a better potential target. The crime of 'cyber extortion' is only studied as it is defined in Chapter II: State of the Art, under *Cyber Extortion and its Manifestations*.<sup>1</sup>

### **Study Methodology**

To complete this study, three specific methods were employed:

- Review of current data regarding transnational extortion. This review includes criminal cases, academic writings, and press publications.
- Personal interviews, including security specialists, law enforcement, legal counsel, industry associations.
- Survey of potential at-risk organizations. The survey was available in two formats – as an electronic form available for completion on the study's web site, and as a Microsoft Word form downloadable from the same site, to be returned via electronic mail or postal service.

## **CHAPTER II: State of the Art**

One of the main difficulties in researching the topic of transnational cyber extortion is the fact that very little research or writings exist on this topic. Understandably, if we assume extortionists use tactics intended to shame or damage the victim into capitulation, we can further assume a victimized organization would not readily report the crime to the authorities, as this could possibly make their security shortcomings a matter of public record. Although the dearth of published research into

---

<sup>1</sup> To be clear, we do not want to confuse cyber extortion with other forms of fraud perpetrated over the internet.

this topic presents a roadblock, the information security and criminology communities have created a wealth of information regarding criminals and the furtherance of their crimes via information systems. Using these resources, we can approach the topic of cyber extortion from a parallel line of study.

### **Cyber Extortion and its Manifestations**

The terms *extortion* and *blackmail* are often used interchangeably when discussing this crime. But, according to Grabosky, et. al. extortion is sometimes defined where the action threatened is independently *illegal* (pay money or bodily harm results), but blackmail when the action threatened is independently *legal* (sign a business deal, or embarrassing photos are sent to the press). [3] This is an important distinction for understanding of this research – the guidelines presented later in this paper intend to aid organizations that operate within the confines of the law, but find themselves potential victims of an *independently illegal* extortion threat. The February 2004 MyDoom virus DDoS<sup>2</sup> attacks against the Recording Industry Association of America (RIAA) present an excellent example. The *legal* request: stop prosecuting people that share music on the internet. The *illegal* threat: a crippling DDoS attack will be launched against your WWW presence if you do not comply. The RIAA did not comply, and as a result their website became inaccessible as the attack commenced.

But are WWW sites, or other customer-facing mediums the only targets of extortionists? Grabosky identifies five manifestations of cyber extortion:

- **Information systems as the medium of threat:** Simple use of computers and networks in the furtherance of an extortion attempt.
- **Information systems as the target of threatened actions:** One of the main concerns facing anyone at risk to cyber extortion. Destruction of data, defacement of websites, or theft of electronically stored intellectual property, if credible, all pose

---

<sup>2</sup> DDoS: Distributed Denial of Service – Using numerous independent computers, a type of attack on a network that is designed to bring the network (or a target computer) to its knees by flooding it with useless traffic

serious threats. Many corporate websites have been targeted, with threats made to post defamatory information on public figures. [4]

- **Information systems as media to disclose embarrassing information:** This could cause particular grief for non-profit or social groups that strive to maintain a spotless reputation in order to conduct their business. Placement of illicit materials on their information systems, followed by an anonymous tip to local newspapers could lead to public condemnation of the organization.
- **Information systems as the means of facilitating payment:** In an electronic world, money changes hands electronically. Specifically, extortion payments are made not in person, but via bank transfers. Grabosky notes the transnational aspect: "Jurisdictions which are hostile to one's own nation would be less inclined to cooperate in a criminal investigation (by not assisting in the identification of the account-holder or the freezing of assets). The very lack of laws or machinery for criminal investigation in a different nation may hinder the cooperation to the extent that the offender may elude investigative authorities."
- **Information systems as incidental to the offense:** Websites and publicly accessible databases house large, albeit not complete, information regarding individuals. This information, if compiled properly across multiple sources, can be used to create personalized threats.

### **Cyber Extortionists**

The processes of economic globalization, which are being facilitated by new information-technology-communications companies, not only provide opportunities for the profitable development of international informational markets, but also simultaneously raise the specter of new criminal activities arising to exploit them. [5] What does this mean? Threats no longer come from our neighborhood, state, or even country. Common sense could lead us to assume the threat of cyber extortion may thrive in countries that do not have the laws in place to outlaw digital crimes, or the manpower and training required to successfully bring extortionists to justice. It goes without saying that the reach of the internet allows organizations worldwide the opportunity to be

victimized with relative ease. This is a profound change in the nature of crime, as the existence of information systems and networks now makes criminal acts possible that were not before, both in increased scope and ease.

Arguably, the most dangerous form cyber extortionists can be defined as *Information Merchants*. These individuals are differentiated from hackers and script-kiddies by security authors Douglas Thomas and Brian D. Loader as: "people [who] trade in the commercial sale of information, engaging in crimes such as corporate espionage and sabotage, sale and theft of identity information, computer and network break-ins, and large-scale software piracy. While they may use similar tools and techniques as hackers, information merchants and mercenaries are primarily driven by profit." [6] Ledeneva agrees, noting a division in the computer antiestablishment: the unstructured underground consists largely of ego-oriented and attention-seeking adolescents and the structured threat that comes from profit-oriented and highly secretive professionals. [7]

### **Eastern European Cyber Criminals**

Turning for moment to the international aspect, we need to examine the phenomena of Eastern European economic crime, specifically the Russian hacker. We look at this particular geographical area only as a starting point due to the many news reports pointing to Russian criminals as the perpetrators of internet extortion attempts. As we progress, we'll revisit the perception created by press reports that Russia and East Europe are hot-beds of cyber extortion.

Data involving international cyber-criminals is typically presented in, and quoted from, the international press as opposed to foreign law enforcement agencies. Why? Crime statistics are determined, according to Ledeneva, "by the efficiency of the legislation and the law enforcement institutions, qualities of control and registration of crime, characteristics of the criminal code, as well as political pressures and influences." [8] Therefore, crime data in the Russian Federation is difficult to obtain and sometimes questionable in terms of accuracy; understandably so, as Russia has been burdened with political and legal scandals since the fall of the Soviet Union.

A fundamental difference between Russian and Western hackers is noted by Rohozinski, in that most Russian hackers tend to be professionals with formal education or work experience involving information technology. Few individuals possess the leisure time or resources to learn hacking as a 'hobby' as is the case in the West. [9] But why would professionals turn to criminal activities? This can be partially explained by the existence of black markets and oppressive social structure in the former Soviet Union. According to Ledeneva, the Soviet regime was known for generating the most skilful, sophisticated and spiritual dissent in every field, normally achieved without opposing the regime in an open way. It is not, therefore, surprising that computer officers could combine their occupation with hacking and achieve exceptional skills which made them in great demand in Russia and abroad. [10]

### ***U.S. Legal Remedies and the Control of Extortion***

As opposed to the lack of published research material on cyber extortion, United States law does specifically address cyber extortion. Considering the multifaceted nature of this crime, its prosecution could be carried out under computer fraud and expanded under other laws separately dealing with the elements of the cyber extortion scheme: the illegal use or access of information systems, denial of service, illegal use of or trafficking in access devices (passwords) and the threat of damage against a potential victim, to name a few.

Specifically, 18 USC §1030, "Fraud and Related Activity in Connection with Computers", addresses these criminal activities. Subsection (a)(7) reads:

*"[Whoever] with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce and communication containing any threat to cause damage to a protected computer [Shall be punished as provided in subsection (c) of this section]"*

This section deals specifically with the treat of damage, a single element in an extortion scheme. As we've discussed, damage to an information system is not the only method to extract consideration from a victim. Subsection (a)(4) of the same U.S. Code states:

*"[Whoever] knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period... [Shall be punished as provided in subsection (c) of this section]"*

An excellent example of the adaptability of this code, the above section tackles the more over-reaching issue of illegal access to a computer in the furtherance of fraud. 18 USC §1030 continues to address various other fraud activities against private and U.S. Government computers and punishment for offenses. For more detail, please refer to the entirety of 18 USC §1030.<sup>3</sup>

### ***International Legal Considerations***

Continuing with legal protections, but with an international perspective, Margaret Jackson notes three main legal approaches companies can employ to protect their information: In Commonwealth countries, like Australia, the United Kingdom and Canada, criminal law, contract, equity and copyright are the main areas of law which provide measures by which a business organization can protect its information from others. Also, in many cases, government officers and those working in particular fields, like health care and telecommunications, are prohibited from disclosing information by numerous secrecy and confidentiality clauses contained in statutes. [11] This provides methods other than reactive legal prosecution to ensure intellectual property and customer records, amongst other data, are kept legally protected.

Cooperation between law enforcement agencies internationally involves "requests under mutual legal assistance treaties (MLATs), letters rogatory<sup>4</sup> in the absence of a treaty or executive

---

<sup>3</sup> See: [http://www.usdoj.gov/criminal/cybercrime/1030\\_new.html](http://www.usdoj.gov/criminal/cybercrime/1030_new.html)

<sup>4</sup> Letter Rogatory: an instrument sent in the name and by the authority of a judge or court to another, requesting the latter to cause to be

## CHAPTER III: Survey Methodology

agreement, and subpoenas directed to U.S. citizens and permanent residents of the United States abroad.” [13] According to Susan W. Brenner and Joseph J. Schwerha IV, the procedure for obtaining assistance under a MLAT is generally faster and more reliable than the older process of using letters rogatory. [14] To further delve into the specific legal strategies for tracking criminals and legal channels to obtaining evidence could constitute another entire paper, and therefore will not be discussed further here.

The above clearly shows that, at least in the United States, we have laws in place to give remedy to acts of cyber extortion, fraud, theft, etc. But, as Grabosky, et. al., note “It is not so much the substantive criminal law, but rather the tasks of detection and investigation, which constitute the greatest challenges for the control of digital extortion.” [12] Investigation of a transnational crime is no simple undertaking, particular against a professional information merchant using technological means to cover their tracks. Grabosky notes that law enforcement’s particular challenge is to identify and locate the extortionist, and take him into custody before the threat can be carried out. If not possible, minimize whatever harm may occur from the threat, and arrest the extortionist(s) as soon as possible thereafter.

Suffice it to say, as well put by Grabosky et. al., extortionists may be serial offenders, as with the case in conventional crime, evidence left at a crime scene may enhance the investigation capacity of the police in another matter. It is therefore no less desirable in circumstances of digital extortion that in other forms of electronic theft that victims are encouraged to report incidents. Discreet management of this information by public authorities is therefore essential.

---

examined, upon interrogatories filed in a cause depending before the former, a witness who is within the jurisdiction of the judge or court to whom such letters are addressed. In letters rogatory there is always an offer on the part of the court whence they issued, to render a similar service to the court to which they may be directed whenever required.

A significant portion of this study revolves around generating statistical data regarding not only the occurrence of cyber extortion, but also small and medium sized organizations’ perception of this crime, and any steps they may have taken to protect themselves. A three part survey was designed and released in order to gather this data. The data itself was analyzed by the author and a number of the strategic partners from law enforcement and information security professions, as mentioned in the acknowledgments.

### ***Subject Selection and Description***

As noted in Chapter I – Limitations of the Study, the survey is intended for SMOs<sup>5</sup>, with less than approximately 10,000 full time employees. This group is selected to not only narrow our focus, but also to follow the assumption that large corporations may have significantly different legal, financial, and political means at their disposal to deal with cyber extortion. Participants, as self-identified in the demographic section of the survey, come from numerous sectors: security, health care, non-profit, business associations, telecommunications, and education, to name a few.

The survey participants were self selecting in that they anonymously volunteered to take part in the study. As noted above, the survey is intended for a specific set of participants, but since submission was anonymous the assumption that each individual response qualifies for participation cannot be independently verified. Great care was taken by the author to inform potential participants of the qualifications for completing the survey. Additionally, any direct contact made to potential participants was limited to those known to be qualified to participate.

### ***Data Collection Procedures***

The survey itself was available at the study’s web site<sup>6</sup>, hosted at Carnegie Mellon University. At this site, participants had the option of completing the survey on-line, via a web submission form, or downloading a copy of the

---

<sup>5</sup> SMO: Small and Medium Sized Organization

<sup>6</sup> <http://www.andrew.cmu.edu/user/gbednars>

survey itself and returning it via email or postal service. All submissions from the on-line web form were sent directly to the author's e-mail account. Once the data was collected it was compiled in a relational database for future analysis.

The survey is included in Appendix A.

### Data Analysis

Following the closure of the survey, the data was reviewed by the author for consistency. Individual responses were checked for data errors by the author (e.g. incomplete responses were discarded), but pursuant to the study's privacy policy, at no time were individual responses reviewed for use in the study; all data was analyzed together after collection was complete.

The data was then analyzed by the author and database queries generated to highlight significant findings and patterns. This was reviewed by the study's advisor and strategic partners, generating the below chapter on discussion.

### Limitations

The survey was made available for participation via the study's web site from July 6, 2004, through August 23<sup>rd</sup>, 2004; all collection was limited to this time. The call for participation was limited to qualified candidates (see above) and achieved through cost-free methods such as industry association newsletters, press releases to newspapers, and direct e-mailings. The research work itself was limited to the time between June and September 2004.

## CHAPTER IV: Results

To truly understand the threat of cyber extortion, we need to look at organizations that may be at risk, measures they have taken (or not taken) to protect themselves against this crime, and review any experiences they may have had with cyber extortion. As noted above, a survey was conducted between July 6<sup>th</sup> and August 23<sup>rd</sup>, 2004, in order to obtain the following data. Chapter IV intends to present the author's findings, and present minimal observations regarding implications. Chapter V: Discussion, will delve deeper into the implications of these results, as well as examine data specific to

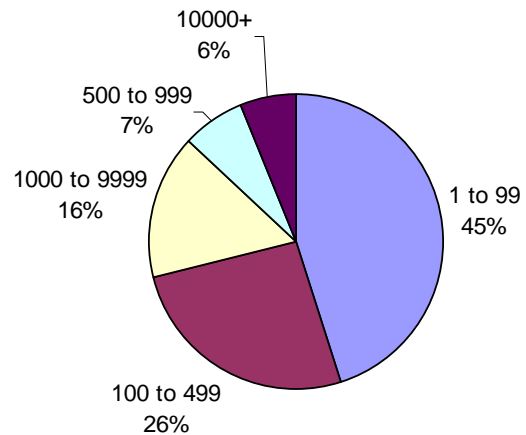
organizations perceiving themselves at "low risk" of cyber extortion.

Exactly one-hundred organizations participated in the study. Unless specifically noted, all results shown in below sections one, two, and three are representative of the full surveyed group.

### Section 1: Demographics

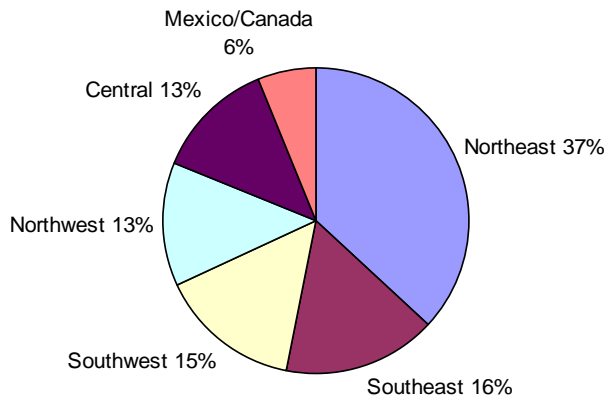
Section 1 aims to gather general demographic information on participating organizations. This data is useful to determine differences (if any) between how different sized organizations understand and deploy information security measures, and how customers and employees access data within the organization. Additionally, we strive to understand what portions of these organizations are required by law to comply with various federal acts regarding the protection of personal data and accurate reporting.

Illustration 1: Approximately how many full-time equivalent employees does your organization employ?



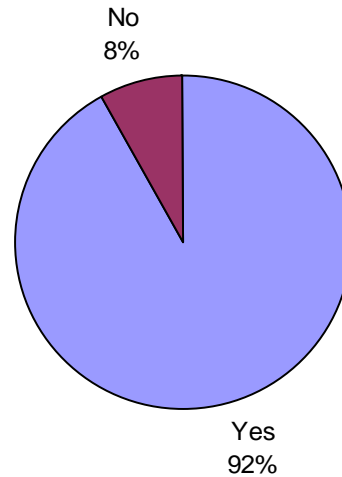
**Illustration 1:** The survey was designated for small and medium sized organizations; those with less than approximately 10,000 full time employees. Although a very small portion of respondents are considered large organizations, the bulk of responses (71%) came from organizations with 1 to 499 employees, and almost a full quarter (23%) from organizations employing 500 to 9,999 employees.

Illustration 2: Which geographic location are you located?



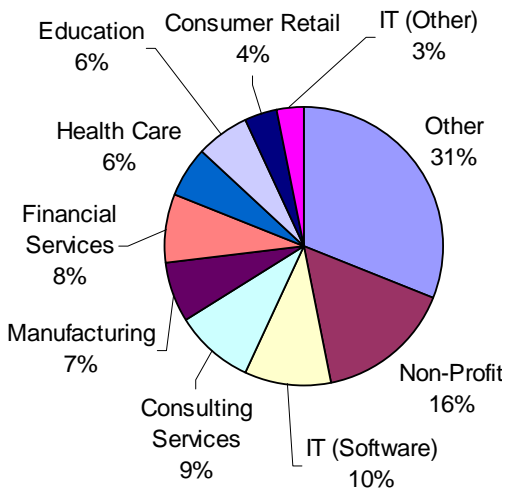
**Illustration 2:** Although the risk of cyber extortion does not depend on the physical location of your organization, this shows the distribution among various regions of the United States and North America, demonstrating a large geographical dispersion of participants.

Illustration 4: Does your organization maintain a WWW presence?



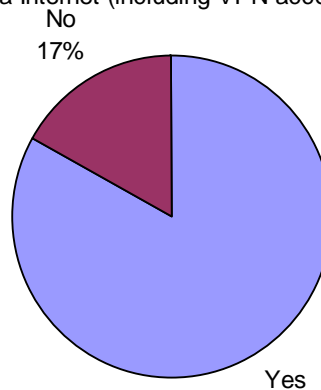
**Illustration 4:** The majority of respondents maintain a presence on the World Wide Web. Although the existence of a WWW presence does not strictly increase the likelihood of cyber crimes against an organization, it does offer a target for criminals – the WWW site is often a customer-facing medium, and commonly targeted for defacement or DoS attacks.

Illustration 3: Your industry?



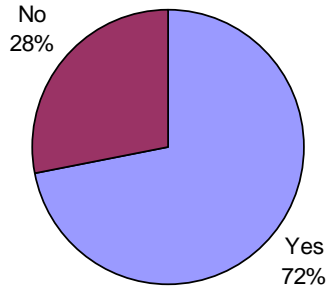
**Illustration 3:** The 'Other' category includes Marketing/PR, Business to Business, IT Hardware, 2% each; Aerospace & Defense, Telecommunications, Legal, and Arts & Entertainment, 1% each. As we will see, organizations in all sectors are potential targets of extortion threats.

Illustration 5: Do you allow employee access to organization intranet/information resources via Internet (including VPN access)?



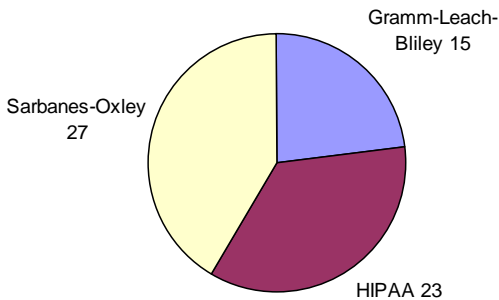
**Illustration 5:** Access to internal organization data from off-site locations, such as telecommuting, by employees. If improperly managed, this may present a direct route into your protected systems for intruders.

Illustration 6: Do you allow client or customer access to organization information resources via the Internet (including online ordering, catalogs, etc.)?



**Illustration 6:** Access to internal organization data by customers or clients. Includes access to ordering and status systems – this internal data that may not be protected as well by clients and customers, as opposed to employees.

Illustration 7: Is your organization required to comply with standards in any of the below acts?

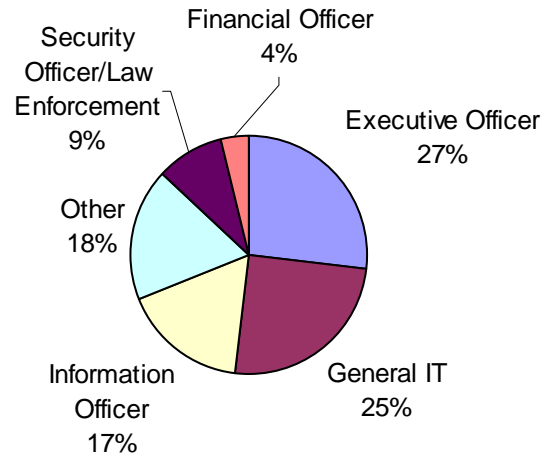


**Illustration 7:** A single organization may have to comply with multiple privacy standards. Having a breach of sensitive data could intensify an extortionist's threat.

**Base:** 40 organizations.

**Note:** Multiple responses allowed.

Illustration 8: What best describes your role within your organization?

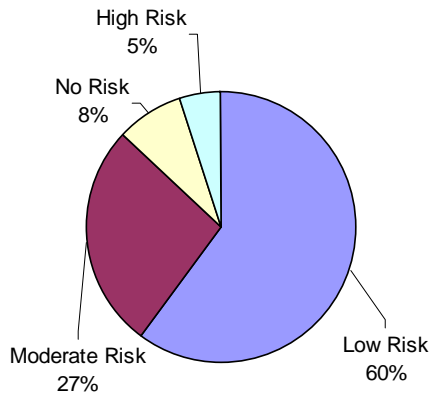


**Illustration 8:** The majority of respondents (27%) are at the executive level of their organization. Information Technology and Information Officers comprised 25% and 17%, respectively.

## Section 2: Cyber Security Preparedness

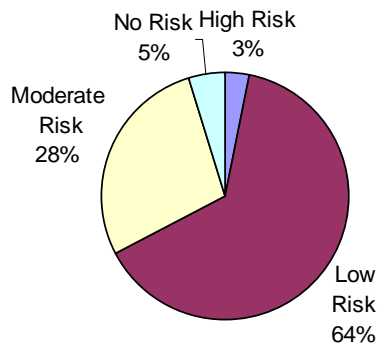
The second section of the survey deals with organizations' actions taken to help reduce the threat of cyber extortion. Although multiple questions ask if specific technological security measures are in place, this does not imply these measures are a complete safeguard against extortion attempts. A portion of this study will generate guidelines useful to business in protecting themselves against extortion attempts. To create these guidelines, we must first understand the level of potential risk and current protection existing in organizations.

Illustration 9: What degree of risk do you believe your organization is at regarding cyber extortion?



**Illustration 9:** Almost two-thirds of respondents believe themselves at low risk of extortion. We examine this particular group in greater detail in the following chapter.

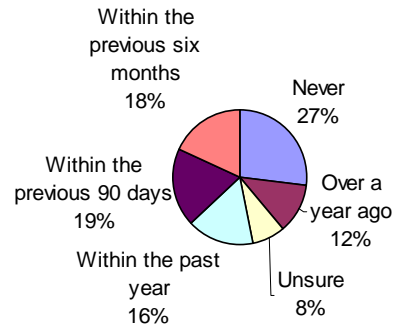
Illustration 10: What degree of risk do you believe your organization is at regarding cyber extortion?



**Illustration 10:** This question is specific to those organizations that maintain a WWW presence and allow clients and employees access internal data from remote locations (see illustrations 4, 5 and 6, above). Notice how this group of 64 organizations' responses show essentially little difference when added to the entire survey group, as in Illustration 9.

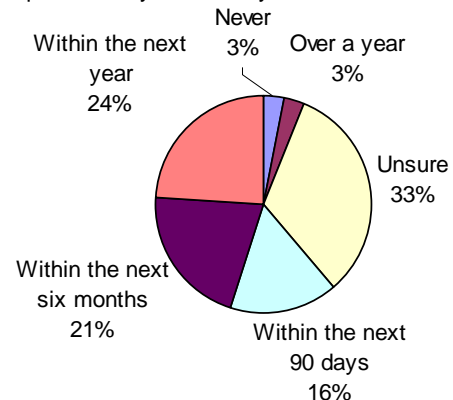
**Base:** 64 organizations.

Illustration 11: When was the last time your organization performed a cyber security risk assessment?



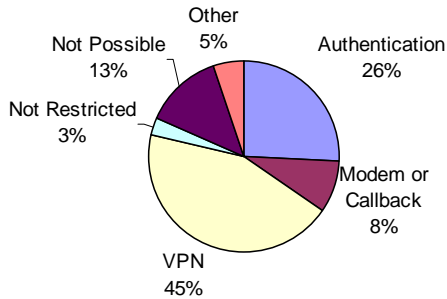
**Illustration 11:** One of the most important actions any organization can take is that of assessing what their most valuable information assets are, and how vulnerable to attack they may be. Just over half of the respondents performed a risk assessment within the past year. Over a full quarter never have.

Illustration 12: When is the next time your organization will perform a cyber security risk assessment?



**Illustration 12:** A potential sign of increasing security awareness, 61% of respondents will perform a risk assessment within the next year, the next six months, or the next ninety days. Note only 3% do not plan to perform an assessment, hopefully reducing the number of "never" responses in Illustration 11 in the future.

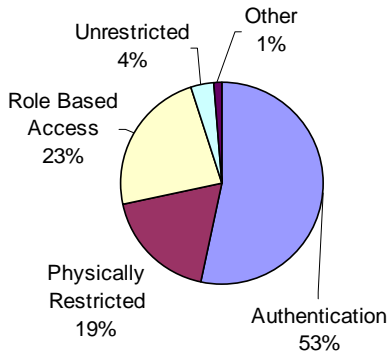
Illustration 13: Describe how sensitive organizational data is accessed externally via your information resources:



**Illustration 13:** Virtual Private Networks (VPNs, sometimes referred to as IP Extension Services) are the most popular form of securing access to internal data from external locations. VPNs typically require some form of authentication, and are typically capable of encrypting transmitted data.

**Note:** Multiple responses allowed.

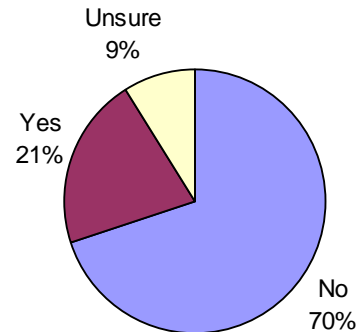
Illustration 14: Describe how sensitive organizational data is accessed internally via your information resources



**Illustration 14:** While on-site, authentication (passwords, etc.) is the most common method used to grant access to specific levels of data. Role based access, grouping users into functional roles and granting access based on those roles, accounts for nearly one-quarter of responses.

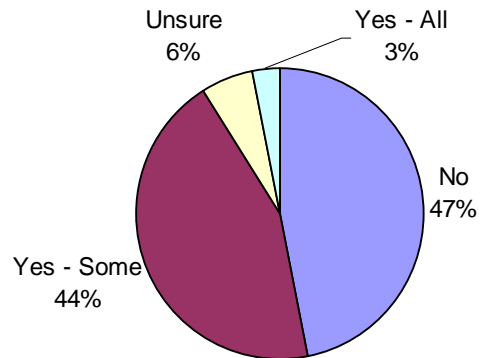
**Note:** Multiple responses allowed.

Illustration 15: Does your organization maintain a standard policy for encrypting sensitive data?



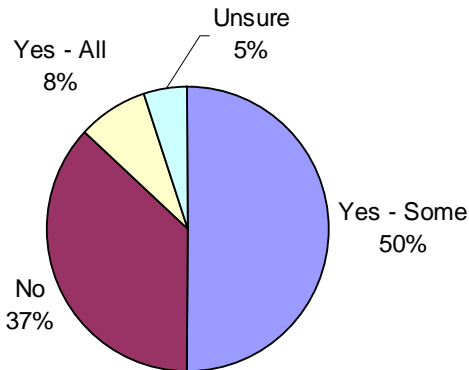
**Illustration 15:** Encrypting data is a useful method of protecting communications and stored information. Without a standard policy of when and where to employ encryption, as well as what encryption is appropriate, could lead to spotty or inappropriate use, weakening the level of protection the encryption may be able to provide.

Illustration 16: Is your organization's sensitive data stored in an encrypted state?



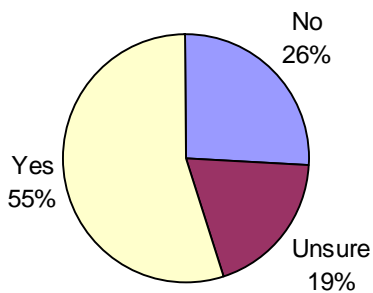
**Illustration 16:** *Stored data is typically the target of theft.* Intellectual property, customer records, sales, financial, and business plans, depending on their level of sensitivity, would be well protected if stored in an encrypted state. Unless an intruder has the correct key(s) to decrypt, any stolen data is essentially useless.

Illustration 17: Are communications with customers or suppliers conducted via secure methods, such as SSL, encrypted email, etc?



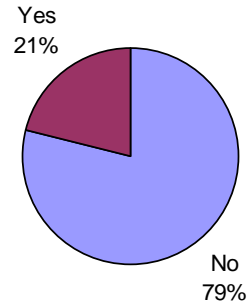
**Illustration 17:** According to the 2004 InformationWeek Global Security Survey [15] two-thirds of the surveyed companies opt for SSL to secure communications. This may lend a false sense of security, since, according to the same survey, the majority of intrusions are reported from compromising known vulnerabilities in operating systems and software, not data in-transit.

Illustration 18: Is your information systems department qualified to respond in cases of an information security incident?



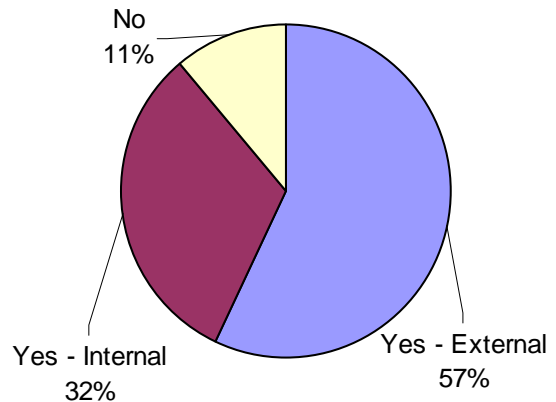
**Illustration 18:** Individuals qualified to quickly find and correct vulnerabilities are necessary to maintaining any secure system. These individuals may also be responsible for configuration of the security systems from the onset.

Illustration 19: Does your organization have a formal training process for employees for what to do in case of an information security event, including extortion?



**Illustration 19:** Personnel training and awareness campaigns are an important facet of an overall security policy as not all threats are technical. Social engineering<sup>7</sup> is a popular and very effective tactic used to obtain data by employing little or no technical means. If employees lack understanding of the threats information merchants pose, they may easily be the weakest link in your proverbial security fence.

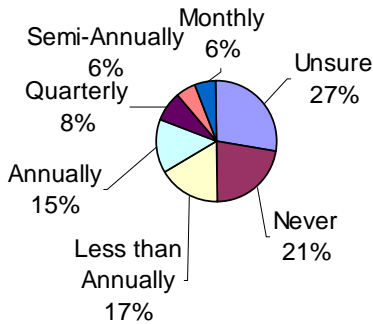
Illustration 20: Does your organization retain legal counsel?



**Illustration 20:** Legal counsel can provide a wealth of advice and protection. Companies may be exposed to downstream liability issues if parties are damaged due to data theft and/or extortion from your information systems.

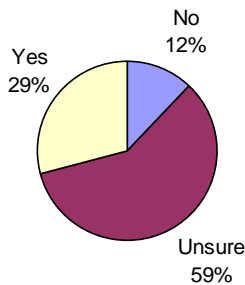
<sup>7</sup> Social Engineering: The practice of conning people into revealing sensitive data on a computer system.

Illustration 21: How often does your organization consult with legal counsel regarding information privacy and/or protection readiness?



**Illustration 21:** Consultation with legal counsel competent in the area of electronic crime law is an excellent addition to any risk assessment. Of those that retain legal counsel, 21% never discuss electronic crime matters, while 17% discuss these issues less than annually.  
**Base:** 89 organizations.

Illustration 22: Is your legal counsel qualified to advise in the case of an information security incident?



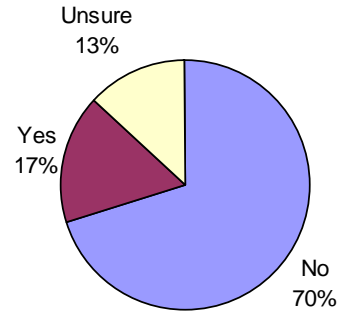
**Illustration 22:** 12% of the study’s respondents are sure they have inadequate legal counsel to handle information security matters. A large majority, 59%, are unsure. Surprisingly, a large number of respondents would turn to their legal counsel first in the case of an extortion attempt (see Illustration 32). This fact is revisited below.  
**Base:** 89 organizations.

**Section 3: Cyber Extortion**

The final section presents data specific to cyber extortion experiences, contacts which would be made in the case of a hypothetical extortion attempt, and organizations risk-tolerance against this crime. Illustrations 24 through 30 are specific to organizations that have had extortion

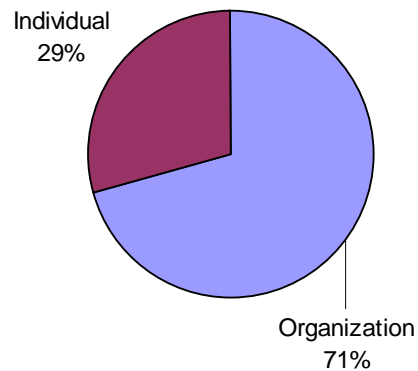
attempts made against them, and are therefore limited to those participants answering “Yes” in Illustration 23.

Illustration 23: To the best of your knowledge, has your organization or an employee of your organization had a cyber-extortion threat made against them?



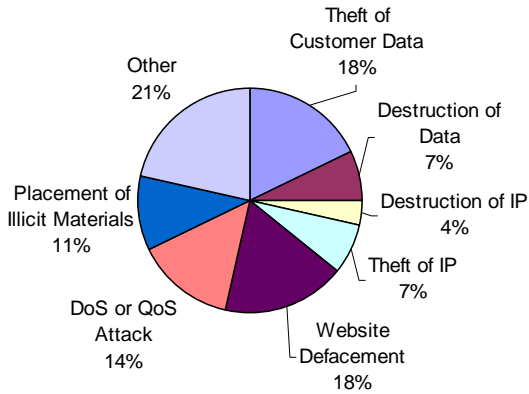
**Illustration 23:** 70% of responding organizations believe they have not had a cyber extortion attempt made against them. If any threats were made against a single employee, or contained embarrassing content, can we hypothesize some threats have gone unreported? In this case “Unsure” may be the most appropriate response.

Illustration 24: Was the threat made against the organization or an individual?



**Illustration 24:** 29% of respondents reporting a cyber extortion attempt note the target victim was an individual, as opposed to the entire organization. Employees fear losing credibility, job status, or being held liable for losses, and may present easier targets than entire organizations.  
**Base:** 17 organizations.

Illustration 25: What was the substance of the threat?

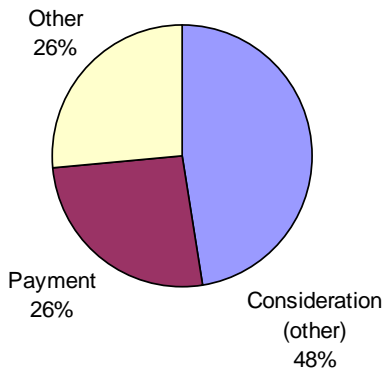


**Illustration 25:** Theft of data<sup>8</sup>, DoS/QoS attacks, and website defacement are the most popular methods used by extortionists. Placement of illicit materials (11%) highlights the tactic of using embarrassment or fear of public scrutiny to succeed in the attempt. The ‘other’ category includes threats such as online smear campaigns and threats of system compromise.

**Base:** 17 organizations.

**Note:** Multiple responses allowed.

Illustration 26: What was the goal of the extortion attempt?



**Illustration 26:** The majority of those reporting extortion attempts note the goal included

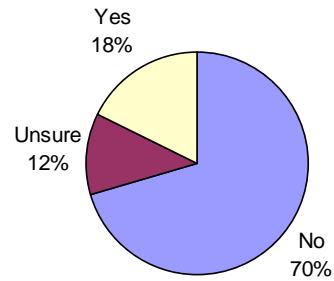
<sup>8</sup> We differentiate between *theft* and *destruction* of data here – theft compromises copying data for potential release, whereas destruction entails complete erasure or corruption of the data with no recovery. Additionally, intellectual property (IP) is separated from customer data and ‘other’ sensitive data to highlight research as a target, as opposed to financial, market, or customer data.

favorable consideration other than payment of money.

**Base:** 17 organizations.

**Note:** Multiple responses allowed.

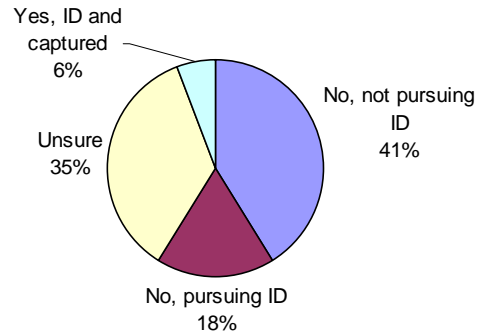
Illustration 27: Was the extortion threat successfully carried out? That is, did the extortionist attain the goal of the threat, regardless of if they were later identified by authorities?



**Illustration 27:** Most threats were not successfully carried out, although the following illustration shows few are being actively pursued. This offers little incentive for criminals to avoid this practice.

**Base:** 17 organizations.

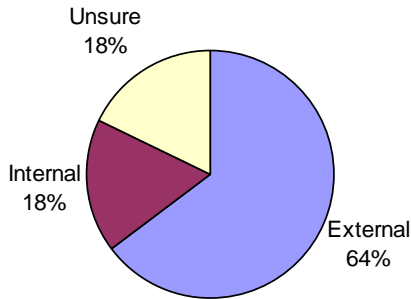
Illustration 28: Was the extortionist identified and/or captured (regardless of if the extortion attempt was successful)?



**Illustration 28:** 41% of respondents reporting attempts are not pursuing identification, while 35% are unsure of the status of their dealings with the attempts.

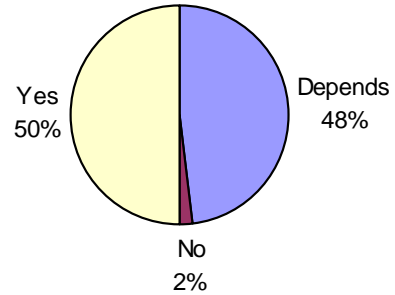
**Base:** 17 organizations.

Illustration 29: Did this threat originate from someone internal or external to the organization?



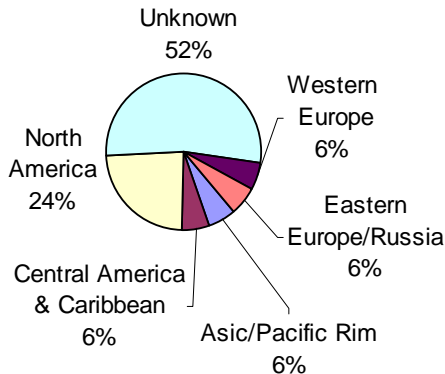
**Illustration 29:** Not all threats originate from outside your organization. In the first Insider Threat Study focusing on the banking and financial sectors, CERT/CC and the U.S. Secret Service have found<sup>9</sup> 87% of insider threats employed simple, legitimate user commands, and 78% of insider cases involved authorized users with active accounts [16].  
**Base:** 17 organizations.

Illustration 31: If your organization had a credible extortion threat made against it, would law enforcement be called to investigate?



**Illustration 31:** According to personal interviews with Federal law enforcement, not reporting these crimes is worse than any fears you may have regarding involvement with enforcement representatives. Legal counsel unequipped to consult in these matters may additionally hinder successful tracking and prosecution of would-be extortionists.

Illustration 30: If the threat originated externally, from what geographical region did the extortion attempt originate?



**Illustration 30:** Although the majority of threat origins have not been geographically pinpointed, North America constituted the next majority of threat origin – this is a significant departure from anecdotal accounts found in the international press. Typically noting Eastern European criminals, only a single identified response came from that geographic location.  
**Base:** 17 organizations.

Illustration 32a: 1st to Call in Response

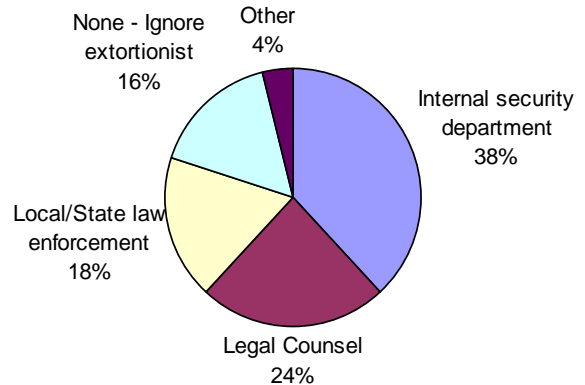
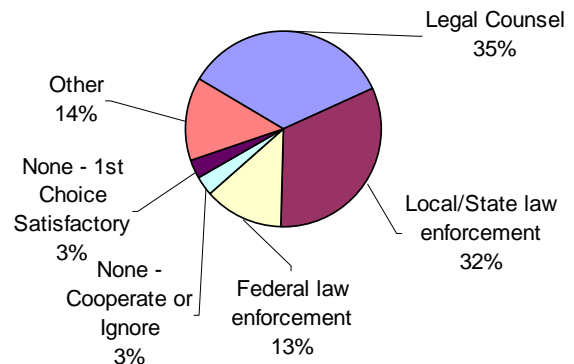
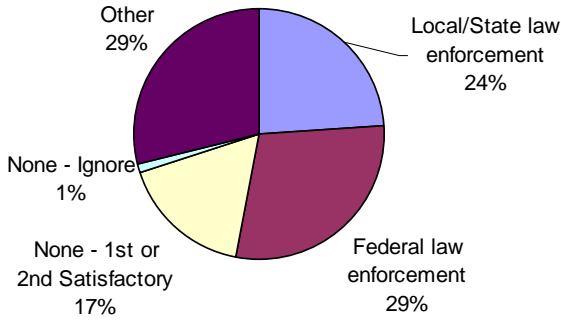


Illustration 32b: 2nd to Call in Response



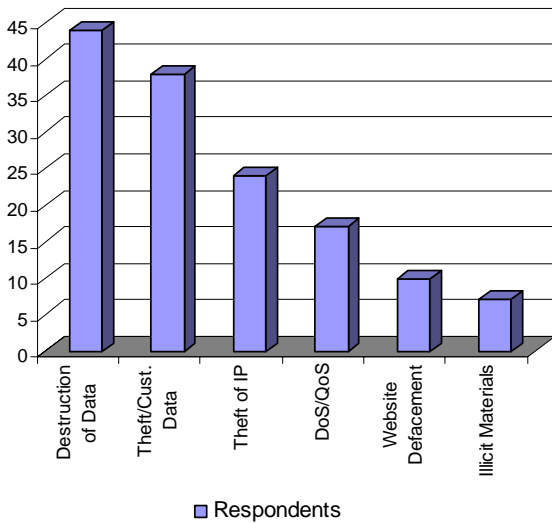
<sup>9</sup> Insider Threat Study findings are not specific to cyber extortion.

Illustration 32c: 3rd to Call in response



**Illustration 32a, 32b, 32c:** Participants were asked who they would turn to for advice and aid in the case of cyber extortion. More importantly, they were asked who would be called first, second, and third. The majority of respondents would contact an internal security department first, followed by their legal counsel. Law enforcement, Federal and local, were last to be called. This is an important distinction, discussed in greater detail below.

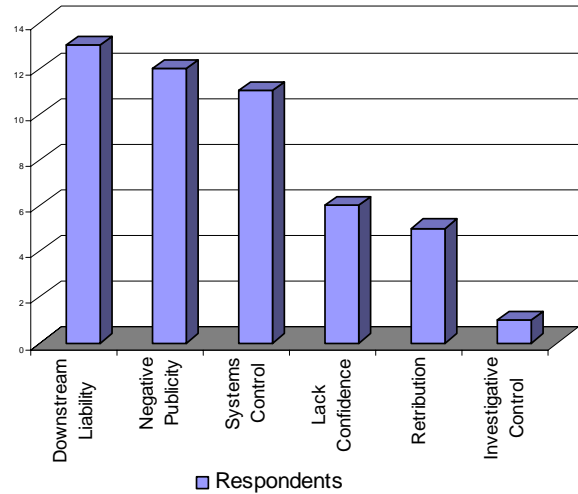
Illustration 33



**Illustration 33:** Participants were asked to rate the above threats on a scale of 1 (non-issue) to 5 (most damaging) in potential to harm their organizations. Illustration 33 shows the number of respondents that have ranked each threat as 'most damaging'. Understandably, destruction of data poses the most serious threat, followed by theft of customer data and theft of other sensitive non-customer data. Compare this with illustration 25, and we see the extortion attempts detailed earlier involve mostly theft and destruction of data: **the extortionists**

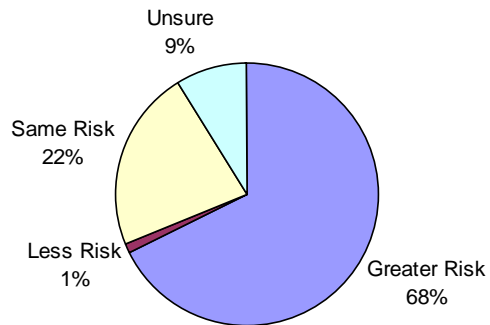
**understand what is of value to organizations, and direct their attacks accordingly.**

Illustration 34



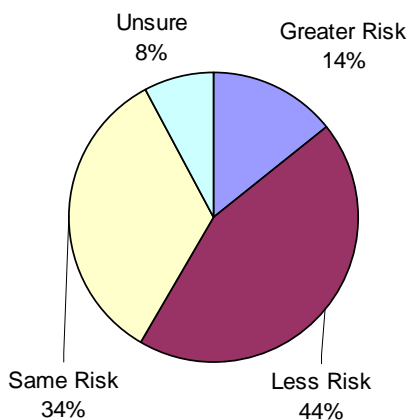
**Illustration 34:** Respondents were asked to rate a collection of reasons as to why they may not involve law enforcement in the case of an extortion attempt. The ratings are in terms of how valid each reason is, and are rated from 1 (not a concern) to 5 (serious concern). The above illustration shows the number of respondents that have ranked each concern as 'serious concern'. Liability for damage to others and negative publicity lead the reasons for excluding law enforcement from dealing with extortion attempts.

Illustration 35: How would you rate the cyber extortion risk potential for organizations that outsource IT and IS functions to non-US regions?



**Illustration 35:** Asking another perception question, most participants (68%) believe outsourcing IT or IS functions to organizations outside the United States pose a greater risk as opposed to domestic outsourcing.

Illustration 36: How would you rate the cyber extortion risk potential for organizations that outsource IT and IS functions to US regions?



**Illustration 36:** Those respondents perceiving offshore outsourcing as a greater risk believe domestic outsourcing presents the same or less risk for domestic outsourcing. The same and greater risk category increases can be explained if some organizations see risk in outsourcing, regardless to the location the work is outsourced.

## CHAPTER V: Discussion

You thought your organization was safe. After consulting with the IT department, you now understand the firewall was somehow circumvented, and the customer data taken when someone created a bogus company e-mail account, using it to e-mail the data outside the organization to a free (and now abandoned) e-mail address. The IT department recommends contacting federal law enforcement so they can begin tracking the path back to the extortionist. Your boss reminds you that if you contact the authorities and press charges, this intrusion would become public knowledge. Meanwhile, you can't help but wonder how it could have been prevented...

In the introduction we put forth a hypothetical extortion attempt: a credible threat, coupled with a request for a small amount of money. Many questions were asked, none answered. This section aims to confront some of those questions by looking at organizations that have placed themselves in an extortion "low-risk" category, reviewing extortionists' methods, and

exploring some ways organizations may better protect themselves from this crime.

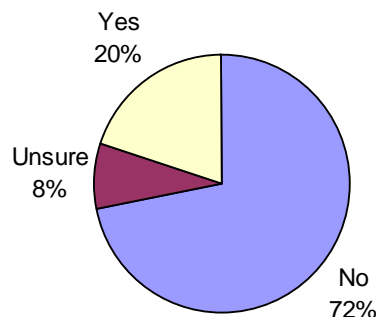
All information presented below, including guidelines and commentary, is not simply the opinion of the author, but the result of numerous meetings with representatives of CERT/CC, The United States Secret Service, the Federal Bureau of Investigation, and specialized legal counsel over the course of this study.

### Low Risk Organizations

Let's first look at those organizations participating in our study who believe themselves at a low risk to cyber extortion. Why is it important to do this? Computer security has fast become an important industry, with many experts and companies selling security devices, software, consultations, and weekend "ethical hacking" classes. While knowing more about security is the first step to protecting yourself, simply deploying firewalls and virus scanners in your organization may create a false sense of security.

The following charts represent answers given by those participants who have placed themselves in the "low risk to cyber extortion" category (see illustration 9). Organizations may place themselves into this category for any number of reasons: confidence in their IS/IT departments, belief they possess no data of value to an extortionist, or maybe they simply don't believe it would happen to them.

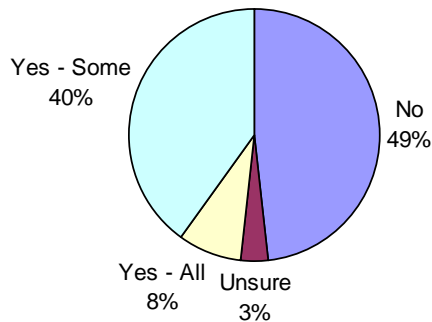
Illustration 37: Does your organization maintain a standard policy for encrypting sensitive data?



**Illustration 37:** 72% of those organizations in the "low-risk" category maintain no standard encryption policy. Encryption can be very useful

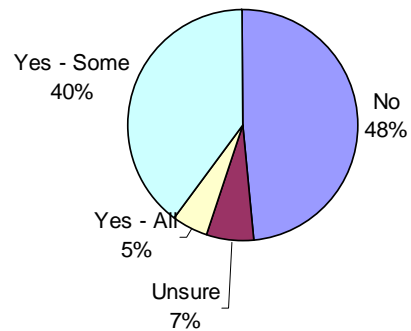
in protecting data from unauthorized access, even in the case of a systems breach, but only if it is applied consistently and correctly. As we see below, 48% of respondents in this category use SSL for encrypting communications, and 45% store sensitive information in an encrypted state. Of those using some type of encryption (approximately 50%), less than half of them maintain a standard policy for its use. Too weak (breakable), too strong (excessive time/processing power used), and applied randomly (encrypted email about fantasy football?) can increase costs and weaken the overall impact encryption can have on the security of your organization.

Illustration 38: Are communications with customers or suppliers conducted via secure methods, such as SSL, encrypted email, etc?



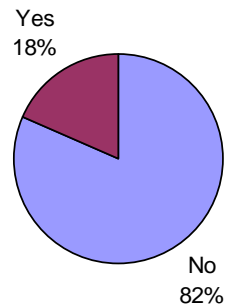
**Illustration 38:** As noted previously, two-thirds of companies surveyed in the InformationWeek Global Security Survey now employ SSL to protect sensitive communications. Less than half of “low-risk” organizations employ this technology for communications with suppliers or customers. While SSL is useful for masking data in transit, the chance of an eavesdropper obtaining any sensitive data while on the open Internet is extremely low. Reported incidents of data theft, including intellectual property and credit card numbers, involve theft from data while in storage, not in transmission, leading us to illustration 39.

Illustration 39: Is your organization's sensitive data stored in an encrypted state?



**Illustration 39:** All too often users believe enormous encryption/decryption keys equal better security. This is not necessarily true – if the underlying algorithm used to encrypt the data is flawed, no key length will offer adequate protection. Aside from right-sizing encryption keys and using the proper algorithms (essential parts of a standard encryption policy) data could be well protected in its stored state using symmetrical encryption. Vulnerabilities in software systems and firewalls may allow for intrusion to your data systems, but if the target information is unusable, extortion involving sensitive data is likely to fail.

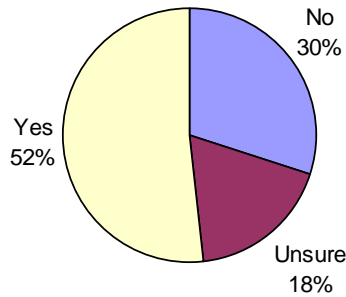
Illustration 40: Does your organization have a formal training process for employees for what to do in case of an information security event, including extortion?



**Illustration 40:** By its nature, cyber extortion is not a strict electronic crime. This crime involves contact between the would-be extortionist and potential victim, transmission and validation of threats, and prying on the victim’s fears in order to make the attempt successful. As we saw in Illustration 24, 29% of respondents that had an extortion attempt made against them claim it was against an individual in the organization. 82% of our “low-risk” group does not maintain

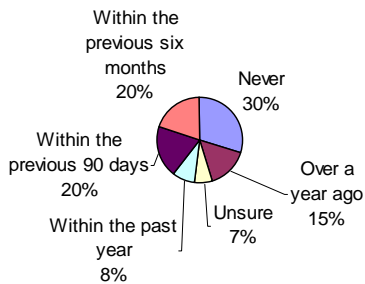
formal training or awareness measures to combat information security events. If individuals in your organization were to be targeted, do you know if they would respond appropriately? Would they alert management, or would they buckle under the substance of the threat, not knowing if they erred and brought this on themselves?

Illustration 41: Is your information systems department qualified to respond in cases of an information security incident?



**Illustration 41:** Technology departments are responsible for a range of duties: set-up, maintenance, patch management, and security, to name a few. How capable do our “low-risk” organizations see their technology departments? Almost one-third (30%) know their IT/IS departments to be unqualified to handle cyber crime issues. Another 18% are unsure their departments are qualified. Note in Illustration 32 most organizations would first turn to their information security departments, possibly unqualified, first in the case of a cyber security intrusion.

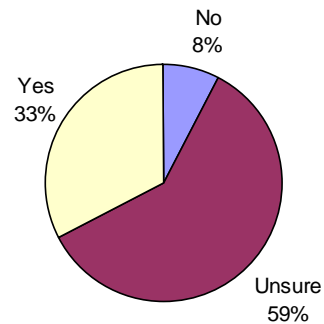
Illustration 42: When was the last time your organization performed a cyber security risk assessment?



**Illustration 42:** Security risk assessments allow management to better understand what is of most value in the information systems –

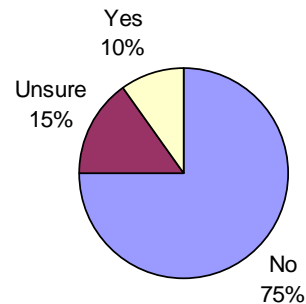
intellectual property, customer records, or perhaps financial data. What systems are most vulnerable? E-mail servers, data repositories, or maybe the online ordering system. *If you don't understand your weaknesses and what is most valuable to your organization, you'll never be able to properly defend your systems.* Luckily, almost half of our low-risk group has performed a risk assessment with the past year, 40% within the past six months.

Illustration 43: Is your legal counsel qualified to advise in the case of an information security incident?



**Illustration 43:** If we revisit Illustration 32, legal counsel is the second-highest and highest preference for who organizations would turn to first and second in the case of a credible extortion attempt (respectively). Yet, almost 60% of our low-risk group is unsure their counsel is qualified in this area. If your legal counsel is unqualified in these matters, what advice will they offer? Will it be correct? Unfortunately, ill-equipped legal counsel could proffer incorrect advice, possibly hindering tracking or prosecution of a criminal.

Illustration 44: To the best of your knowledge, has your organization or an employee of your organization had a cyber-extortion threat made against them?



**Illustration 44:** Some of our “low-risk” group has been extorted! If you have been extorted, it is hoped that every action has been taken to steel your IT and IS systems from repeats of this crime, thereby placing you in a lower risk category.

**Here’s the take-away from this entire analysis: If your organization can identify with even a few of the above illustrations, you are not low risk.** Can we comfortably agree that our self identified low-risk category should remain as such? Not exactly. Depending on the extent information systems are used, a number of factors point to (at least) a moderate risk level for the above organizations.

Few organizations maintain standard policies for use of encryption. This is even the case in organizations where encryption is deployed in customer communications or storage of sensitive data. Encryption is more heavily relied upon for communication, rather than storage, although publicly available accounts point to data theft from storage, not communication, in the commission of extortion attempts.

Serious deficiencies exist in personnel management – both in training and understanding capabilities. If your internal IT or IS department is incapable of understanding the weakness of your information assets, or your employees unsure of how to deal with social engineering or threats made against them, how will they protect themselves and bring issues to your attention? Moreover, how will they protect the data they oversee? Unqualified legal counsel presents a potential to hinder law enforcement’s ability to bring extortionists to justice. Illustrated by a classic example, a company’s counsel is used as a conduit to contact authorities for help in a computer intrusion. To begin the investigation, the law enforcement officials request server logs and records, only to be told by the same counsel the data won’t be shared without a court order!

### ***Extortion Methods***

Understanding methods extortionists use to carry out their crimes is essential to reducing your chance of becoming a victim. Going back to our hypothetical example for a moment, we detail a classic theft of sensitive data case, coupled with a threat to release this data, with

the aim of causing damage to the intended victim’s credibility and customers. This particular method of extortion tied for the most common amongst those study participants who have been extorted in the past – 18% report theft of data or defacement of their website as the substance of the threat, followed by 14% reporting a denial of service or other degradation in quality of service. Keep in mind that these threats may be compound – if an extortionist has access to pilfer sensitive data, they may also have access to modify your website. Let’s review a number of extortion methods, starting with the most commonly reported by our survey group.

**Theft or Destruction of Data:** Reported as the method of extortion by 18% of our extorted participants, the theft threat involves theft of data most commonly associated with customers - credit card numbers, addresses, order histories or forecasts, and contact information. Destruction of data was ranked as the most damaging method an extortionist could use by almost 45% of our total survey group. One of the most reported-on attempts involved a hacker from Kazakhstan, Oleg Zezev, breaking into the computer systems of Bloomberg L.P. Zezev copied credit card numbers and screens relating to internal functions of Bloomberg, as well as various internal information that was only accessible by Bloomberg employees. [\[17\]](#) A request for \$200,000 in exchange for not releasing the information to the media as sent to Michael Bloomberg.

**Website Defacement:** Tied with data theft, website defacement constituted an equal number of threats against extorted participants in our study. This threat may be of particular concern to any organization relying on its ties to community and maintaining spotless reputations to conduct business – non-profit organizations, religious groups, community-based businesses. Anyone maintaining an electronic marketing or information presence on the WWW can quickly find their customer-facing medium pointing to a competitor, advertising obscenities, or clandestinely sending copies of customer log-on information to alternative collection points. While correcting defaced websites can be trivial through use of backups, the damage done to customer confidence or through media coverage could be very critical.

**DoS or QoS Attacks:** Denial of Service (DoS) and Quality of Service (QoS) attacks placed second among respondents, with 14% experiencing this type of threat. A denial of service attack aims to create a load on your information systems so high that they are effectively unusable. When multiple computers are coupled with high-speed connections, any server meant to be accessed over the Internet could be overwhelmed with constant requests to connect (a SYN Flood) or constant requests for large files, such as graphics from a web page (a form of HTTP attack). This could be extremely damaging to any organization conducting commerce via websites or other Internet-enabled systems. Considering the large number of Internet gambling sites that have been targeted by this method, we can practically refer to it as the "Bookie Attack": pay off the extortionists, or you'll have the door to your business blocked until you go broke. Business Week notes "industry experts fear that they [DoS extortionists] could soon target government operations, e-commerce companies, banks -- practically any organization with an online presence." [18] Most recently, the FBI has brought to justice a group using DoS attacks to cripple competitors. FBI Agent Frank Harrill says "This is an example of a growing trend: that is, denial of service attacks being used for either extortionate reasons, or to disable or impair the competition." [19]

How much can this cost your organization? If the aim of this method is to make your servers unusable, according to the Fibre Channel Association downtime hourly costs may amount to those in the table below:

<b>Business</b>	<b>Industry</b>	<b>Hourly Costs</b>
Brokerage Operations	Finance	\$6,450,000
Credit Card / Sales Authorizations	Finance	\$2,600,000
Pay-per-View	Media	\$150,000
Home Shopping	Retail	\$113,000
Catalog Sales	Retail	\$90,000
Airline Reservations	Transportation	\$90,000
Tele-ticket Sales	Media	\$69,000
Package Shipping	Transportation	\$28,000
ATM Fees	Finance	\$14,500

**Placement of Illicit Materials:** Experienced by 11% of those who have dealt with extortion attempts, this threat could be very useful against an individual in an organization, as opposed to the entire company itself. If an employee opens their email to find it bursting with pornography or other prohibited materials, along with a simple request for \$100 to not report this to management, would they be sufficiently shamed into compliance? It's not uncommon that an individual would fear career or social implications even if the material clearly was not theirs.

### **Myths**

Before we can fully discuss how your organization can better protect itself against the threats of cyber extortion, we need to dispel some myths regarding extortion itself, protective technology and law enforcement cooperation.

**Firewalls protect all:** According to the InformationWeek 2003 Global Security Survey, 81% of all participating organizations noted firewalls as a defensive safeguard used, while only 16% of participating organizations reported deploying end-user security training. This is echoed by our own study, as the majority of respondents note firewalls as the best technological method to reduce the threat of extortion, yet illustration 19 shows only 21% having a formal training process for employees to deal with an information security event. Firewalls can only function to the extent they are deployed around the right assets. Additionally, the prevalence of fast spreading worms or viruses distributed via email, some installing backdoors through firewalls, can effectively nullify the usefulness of a firewall.

**Loss of systems control during investigation:** Loss of systems control came in as the third most significant concern by organizations as to why they would not involve law enforcement during an extortion attempt. We're all familiar with video of federal agents hauling computers out of homes and office buildings on the nightly news, and unless you've dealt with law enforcement, it's understandable that this is your only impression of how an investigation is carried out. Not true, as confirmed by both U.S. Secret Service and

Federal Bureau of Investigation agents<sup>10</sup> that have spent the past few years of their careers in their respective cyber crime divisions. Systems disruption typically takes less than an hour, usually involving creating an image of the compromised system's hard drive. System downtime is expected to be low.

**Negative publicity can result through law enforcement involvement:** While criminal cases sent to court are made a matter of public record, victimized organizations may withdraw their request for an investigation before that point. While legal authorities are investigating a cyber crime issue, all details are kept in confidence; facts and comments released to the media can be made by the organization itself. If significant enough, extortion attempts will typically become public knowledge regardless of involvement with law enforcement, as in the case of Japan's Softbank. After police arrested four men attempting to extort the ISP in February 2004, the company admitted it was investigating 242 other instances where customer information was leaked. [20] FBI Agent Thomas X. Grasso notes the best course of action is to cast coordination with the authorities in the proper light: working with law enforcement to better security and bring the criminals to justice. Another option would be explaining a cover-up to your customers and stakeholders...

**All extortionists are from Eastern Europe:** We noted earlier that most accounts of cyber extortion in the international press point to Russian or Eastern European criminals and gangs. Our study has revealed that, of the 17% of respondents having dealt with an extortion attempt, only one of the *identified* extortionists was located in Eastern Europe, equal to those in Western Europe, Central America and Asia. Four times as many originated from North America. Just over half of those responding organizations have not identified the geographical location of the extortion attempts, leaving a large gap for speculation. On another note, 18% of those organizations noted the extortion attempt was an insider threat: someone employed or contracted by them used their access to extort the company. While we cannot definitively say where most extortionists hail from, we do know this crime is truly gaining popularity on a global scale.

---

<sup>10</sup> Obtained through personal interviews with author

**Cooperating with extortionists will make them go away:** Our tragic figure introduced to convey a hypothetical extortion attempt notices the criminals are asking for a relatively small amount of money. Why not pay it? Federal law enforcement agencies agree: pay an extortionist, they'll be back. Many countries have policies of never negotiating with terrorists – consider an extortion attempt terror against your business. Considering the automated nature of some cyber crimes (scripted scanning and vulnerability exploitation), criminals can attempt these threats against a large number of organizations without significant effort on their part. Small ransoms increase the likelihood of cooperation, but cooperation never guarantees the end of extortion.

### **Protective Guidelines**

Computer security is big business – consulting firms, weekend classes, network firewalls and intrusion detection systems. Most of the remedies offered today focus on the technical aspect of keeping intruders out of your information systems, ignoring the aspects of user training and creating proactive incident response plans. Although there is no combination of technologies and policies that can guarantee a completely secure system, ignoring your users, legal remedies, and strategic security planning will leave portions of your organization open to attacks, make damage control more difficult, and extend recovery times, leading to greater productivity and financial losses.

We need to look at security from a more encompassing, strategic perspective to effectively reduce exposure to cyber extortion. This also allows us to respond correctly and efficiently in the case of an extortion incident. You'll notice the following guidelines focus around security policy measures, as opposed to a list of commercial product solutions. A robust, regularly reviewed security policy should be the foundation of any secure information system.

**Security Assessments:** Before any serious security investment can be made, an assessment of your systems' most vulnerable and most valuable points should be created. For cyber extortion, remember data is typically at the heart of the attempt: customer data, financial records, perhaps intellectual property.

Extend the assessment to any potential weak points, including backbone providers – how can they assist you in the case of a DoS attack, and do they maintain logs of system access? Security assessments should be repeated regularly, but particularly when the architecture of your information system changes. Consider this the first step in risk management for your information infrastructure.

**Survivability:** Security is no longer useful after your system has been compromised. Any secure system should be designed to be able to carry on critical services even in the event of a cyber crime. Survivability is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. [21] If a would-be extortionist attempts to hold sensitive data hostage by copying it and deleting it from your server, can you respond with backups of the data? If so, how old are these backups? Other contingencies should be crafted with denial of service attacks, website defacement, and placement of illicit material tactics in mind.

**Plan for a Crisis:** All too often action plans and responses are created after a threat or compromise has been made. Ensure your organization has a written process containing steps to take in the case of a security situation. Planning with a ‘cool head’ will ensure no rash decisions are made under the pressure of a threat.

**User Training and Awareness Programs:** An entire system’s security is only as strong as its weakest link, but oftentimes those who manage the information systems forget it is the user, not the firewall (or IDS, or VPN, or PGP keys, or...) that is most prone to failure. Even with the increased focus on security and its technologies, the rate of cyber security incidents has remained high. Since extortion is one crime with a distinctive human aspect, and can occur against an employee, not only the entire company, one would do well to educate any users with access to sensitive information on how to protect it. Additionally, malicious insiders will be less likely to succeed under the watchful eye of aware co-workers.

**Competent Legal Counsel and Information Systems Department:** Just over one-quarter of our survey’s participants know their information systems departments are ill-equipped to

respond to security events. More concerning is the fact that almost 60% of respondents are unsure if their legal counsel can advise in an extortion matter, but would turn to them first in the case of a cyber security incident. Asking for aid from someone who cannot provide adequate advice is a slippery slope to descend. Bad decisions can lead to angry customers, lost revenues, and untraceable criminals. Have frank conversations with those you rely on to provide legal and technical assistance. If they can’t help, ensure they can produce someone who can if the need arises.

**Law Enforcement Good-Will and Cooperation:** Two federal law enforcement agencies, the FBI and U.S. Secret Service, share jurisdiction for prosecuting cyber crimes across state lines. Additionally, these agencies maintain public-private organizations that aim to increase information sharing between government and private industry, such as InfraGard<sup>11</sup>, and streamlined methods of reporting cyber crimes, such as the Secret Service’s SSF 4017 form for reporting network security incidents.<sup>12</sup> Contact your local Secret Service Electronic Crimes Task Force or InfraGard group before a security incident happens – they can offer advice for best security practices and policies. Finally, you can gain insight as to how they may be able to assist in the case of a security event. State and most local law enforcement agencies also participate in these groups.

## Chapter VI: Conclusion and Future Work

Hopefully this study has raised the visibility of extortion as a cyber crime able to pose significant threats to organizations. Not limited to attacking computer systems, the perpetrators of this crime attempt to defraud targets through threats and intimidation.

We’ve seen there is little research and discussion on this topic; cyber extortion is typically grouped under general “computer fraud” headings, or broken into its component crimes of hacking or electronic theft. We’ve also seen that when taken as a whole, many

<sup>11</sup> For more information on InfraGard, see <http://www.infragard.net>

<sup>12</sup> Form available at [http://www.secretservice.gov/forms/form\\_ssf4017.pdf](http://www.secretservice.gov/forms/form_ssf4017.pdf)

organizations are not well prepared to deal with this blended threat. Opting to rely on intrusion detection and firewall systems, some lose sight of the larger threat facing their organizations. Finally, in the case of a legitimate threat, law enforcement needs to be notified – even if the attempted extortion fails. Many organizations consider not involving law enforcement for a variety of reasons, which exacerbates our lack of data on this crime, not to mention leaves little incentive for would-be criminals to pursue a more legitimate line of work.

A few simple steps can be taken to improve your organization's chances of surviving an extortion attempt. While it is true some of these steps (particularly the security assessment) may lead to larger projects, confronting security shortcomings on both the technology *and* policy fronts can greatly reduce your risk of falling victim to extortionists.

As noted earlier, this study was restricted in a number of ways: language barriers, a short timeframe, and the inherent difficulty of tackling a little understood global cyber crime issue. While this study represents the first step in comprehending and eventually managing this threat, more work can be done. As of this writing, the embassies of numerous Eastern European countries have been unresponsive to requests for data regarding cyber extortion across their borders. Law enforcement and professional associations, although very helpful in this study, need to be involved on a national level to help craft statistics representing a larger sample of organizations, perhaps globally. Personal interviews with extortion victims worldwide and creation of partnerships with private security organizations would lend more insight into the technical details of how threats are carried out, and defended against.

Once the resources and interest exists, we can truly begin to combat cyber extortion, not just respond to its threats. For now, we as businesses, organizations, and individuals must take stock of the shortcomings in our own policies and defenses, as well the organizations that can help, and the options we have if confronted with this crime.

## ACKNOWLEDGMENTS

I would like to express my gratitude to Dr. Jeffrey Hunker for his guidance and helpful

insight during the course of this research. Without the aid of his experience and criticism this research would not have reached its potential.

My special thanks go to InformationWeek Magazine, not only for helping to fund this project through the InformationWeek Summer Research Fellowship, but for lending their namesake to the study itself. Their kind assistance has provided this study with the recognition it otherwise may not have had, greatly encouraging private organizations to share sensitive security data with the author.

Those who I consider strategic partners and counselors in this project: Assistant District Attorney Joseph J. Schwerha IV, Esq. of Schwerha & Associates, for providing legal insight and commentary; United States Secret Service Special Agent Wayne Peterson, Carnegie Mellon SEI/CERT-CC project manager Dawn Capelli, and Federal Bureau of Investigation Special Agent Thomas X. Grasso for their review and analysis of the survey results and creation of policy guidelines. I offer my sincerest thanks for their time, effort and contribution.

To those who made the survey results possible through distribution: InfraGard, The Pittsburgh Technology Council, Greater Pittsburgh Chamber of Commerce/Allegheny Conference, Security Focus, and Professor Michael DeKay for lending assistance in format and creation of the survey. The survey pre-testing group, Don Ojoko-Adams, Jaime Agurello, David Blake, Peter Chen, Jay Miller, and Peter Zeinoun, for taking time to review and comment on the clarity and content of the survey itself.

I would like to thank the Software Industry Center for co-sponsoring the InformationWeek Fellowship, the Information Security Policy and Management administrators, professors, and staff, and Carnegie Mellon's H. John Heinz III School for making my research work possible.

Finally, I would like to thank all those that participated in the study itself – you have provided a valuable and original first insight into the understanding of this crime.

## REFERENCES

- [1] Phil Williams, Casey Dunlevy, Tim Shimeall, "Intelligence Analysis for Internet Security", CERT Coordination Center Research.
- [2] National Hi-Tech Crime Unit, "Hi-Tech Crime: The Impact on UK Business", NHTCU/NOP World Publication, 2003.
- [3] Peter Grabosky, Russell G. Smith, and Gillian Dempsey, *Electronic Theft: Unlawful Acquisition in Cyberspace* (New York: Cambridge University Press, 2001).
- [4] Dorothy Denning, *Information Warfare and Security* (New York: ACM Press; Reading, Mass.: Addison-Wesley, c1999).
- [5] Manuel Castells: *The Information Age: Economy, Society and Culture* (Malden, Mass.: Blackwell Publishers, 1998).
- [6] Douglass Thomas and Brian D. Loader, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age* (London; New York, N.Y.: Routledge, 2000).
- [7] Alena Ledeneva and Marina Krukchiyan, *Economic Crime in Russia* (London; Boston: Kluwer Law International, 2000).
- [8] Ibid.
- [9] Rafal Rohozinski, "Behind the Looking Glass: The Origins, Practices and Daily Life of Russian Cyberspace" (Ph.D. Dissertation, University of Cambridge, 2000).
- [10] Ibid.
- [11] Margaret Jackson, "International Developments to Protect Undisclosed Business Information", in Douglass Thomas and Brian D. Loader, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age* (London; New York, N.Y.: Routledge, 2000).
- [12] Ibid.
- [13] Henry H. Perritt Jr., *Jurisdiction in Cyberspace*
- [14] Susan W. Brenner and Joseph J. Scherha IV, "Transnational Evidence Gathering and Local Prosecution of International Cybercrime", in *Cybercrime, Electronic Warfare & Economic Espionage*, ed. David J. Loundy (Durham, NC: Carolina Academic Press, 2003).
- [15] InformationWeek, "2004 Global Security Survey".
- [16] Carnegie Mellon Software Engineering Institute and United States Secret Service, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector", August 2004.
- [17] U.S. Department of Justice, "Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion" (US DOJ Press Release July 1<sup>st</sup>, 2003).
- [18] BusinessWeek Online, "Gambling Sites, This is a Holdup", BusinessWeek Online, 31 July 2004.
- [19] Kevin Poulsen, "FBI Busts Alleged DDoS Mafia", Security Focus, 26 August 2004.
- [20] iAfrica.com, "Four Nabbed for Internet Extortion", iAfrica.com 01 March 2004.
- [21] R.J. Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T.A. Longstaff, N.R. Mead, "Survivable Systems: An Emerging Discipline," *Proceedings of the 11th Canadian Information Technology Security Symposium (CITSS)*, Ottawa, Ontario Canada, May 10-14, 1999, Communications Security Establishment, 1999.

## Appendix A: Cyber Extortion Survey

Note: Descriptive paragraphs at the start of each section have been omitted for brevity. Terms were defined and instructions were detailed to ensure participants completed the survey correctly.

### Section I – General Demographic Data

Q1: Approximate full-time equivalent employees:

<input type="checkbox"/> 1-99	<input type="checkbox"/> 100-499	<input type="checkbox"/> 500-999	<input type="checkbox"/> 1,000-9,999	<input type="checkbox"/> 10,000+
-------------------------------	----------------------------------	----------------------------------	--------------------------------------	----------------------------------

Q2: U.S. geographic region:

<input type="checkbox"/> Northeast	<input type="checkbox"/> Northwest	<input type="checkbox"/> Southeast	<input type="checkbox"/> Southwest	<input type="checkbox"/> Central
------------------------------------	------------------------------------	------------------------------------	------------------------------------	----------------------------------

Q3: Industry:  
(click to select)

Q4a: Management roles existing within your organization (Check all applicable):

<input type="checkbox"/> Technology Officer (ex: CTO)	<input type="checkbox"/> Info Security Officer (ex: CISO)	<input type="checkbox"/> Information Officer (ex: CIO)	<input type="checkbox"/> Privacy Officer
<input type="checkbox"/> General IT Management	<input type="checkbox"/> Help Desk Management	<input type="checkbox"/> Legal Counsel	<input type="checkbox"/> None of these

Q4b: Roles contracted to external organizations (Check all applicable):

<input type="checkbox"/> Technology Officer (ex: CTO)	<input type="checkbox"/> Security Officer (ex: CISO)	<input type="checkbox"/> Information Officer (ex: CIO)	<input type="checkbox"/> Privacy Officer
<input type="checkbox"/> General IT Management	<input type="checkbox"/> Help Desk Management	<input type="checkbox"/> Legal Counsel	<input type="checkbox"/> None of these

Q5a: Does your organization maintain a World Wide Web presence?

Yes  No

Q5b: Do you allow employee access to organization intranet/information resources via Internet (including VPN access)?

Yes  No

Q5c: Do you allow client or customer access to organization information resources via the Internet (including online ordering, catalogs, etc.)?

Yes  No

Q6: Is your organization required to comply with standards in any of the below acts?

- Sarbanes-Oxley
- HIPAA
- Gramm-Leach-Bliley

Q7: What best describes your role within your organization?

(click to select)

---

### Section II – Cyber Security Preparedness

Q1: What degree of risk do you believe your organization is at regarding cyber extortion?

No risk  Low Risk  Moderate Risk  High Risk

Q2a: When was the last time your organization performed a cyber security risk assessment?

- Within the previous 90 days
- Within the previous six months
- Within the past year
- Over a year ago
- Never
- Unsure

Q2b: When is the next time your organization will perform a cyber security risk assessment?

- Within the next 90 days
- Within the next six months
- Within the next year
- Over a year
- Never
- Unsure

Q3a: Please describe how sensitive organizational data, such as intellectual property, customer, or financial data is accessed externally via your information resources (Check all applicable):

- Access allowed via VPN
- Access allowed via modem pool or call-back
- Access allowed via any Internet connection with proper authentication (e.g. password)
- External access not restricted
- External access to sensitive information not possible (e.g. not connected to network)
- Other:

Q3b: Please describe how sensitive organizational data, such as intellectual property, customer, or financial data is accessed internally via your information resources (check all that apply):

- Access allowed with proper authentication (e.g. password)
- Access only possible via certain physically restricted systems
- Only possible via role-based access
- Access is unrestricted while on-site
- Other:

Q4a: Is your organization's sensitive data stored in an encrypted state?

- Yes – all  Yes - some  No  Unsure

Q4b: Does your organization maintain a standard policy for encrypting sensitive data?

- Yes  No  Unsure

Q4c: Are communications with customers or suppliers conducted via secure methods, such as SSL, encrypted email, etc?

- Yes, all  Yes, some  No  Unsure

Q5: Is your information systems department qualified to respond (identify and correct potential security vulnerabilities, determine the extent of damage) in cases of an information security incident?

- Yes  No  Unsure

Q6: Does your organization have a formal training process for employees for what to do in case of an information security event, including extortion?

- Yes  No

Q7a: Does your organization retain legal counsel?

- Yes – Internal  Yes – External  No

Q7b: How often does your organization consult with legal counsel regarding information privacy and/or protection readiness?

- Monthly
- Quarterly
- Semi-Annually
- Annually
- Less than annually
- Never
- Unsure

Q7c: Is your legal counsel qualified to advise (specialize in or have experience dealing with information security incidents and laws) in the case of an information security incident?

- Yes  No  Unsure

---

### Section III – Cyber-Extortion

Q1a: To the best of your knowledge, has your organization or an employee of your organization had a cyber-extortion threat (as defined above) made against them?

- Yes  No (please skip to question 2)  Unsure

Q1b: Was the threat made against the organization or an individual?

- Organization  Individual

Q1c: What was the substance of the threat? (Check all applicable)

- Theft and release of customer data (credit card data, purchase histories, etc.)
- Theft and release of intellectual property (patents, research, etc.)
- Theft and release of sensitive internal data (human resource, financial data, etc.)
- Placement of illicit materials on organization computer systems
- Defacement of website or other externally-facing medium
- Destruction of any intellectual property, customer data, or other sensitive internal data
- Denial of Service (DoS) attack or other detrimental quality of service measure
- Other:

Q1d: What was the goal of the extortion attempt? (Check all applicable)

- Favorable consideration/action for extortionist
- Change of business plan
- Payment to extortionist monetarily or with products/services
- Other:

Q1e: Was the extortion threat successfully carried out? That is, did the extortionist attain the goal of the threat, regardless of if they were later identified by authorities?

- Yes  No  Unsure

Q1f: Was law enforcement contacted? (Check all applicable)

Type	Timing
<input type="checkbox"/> Local	<input type="checkbox"/> After extortion threat received
<input type="checkbox"/> State	<input type="checkbox"/> After payment made (if applicable)
<input type="checkbox"/> Federal	<input type="checkbox"/> N/A
<input type="checkbox"/> N/A	

Q1g: Was the extortionist identified and/or captured (regardless of if the extortion attempt was successful)?

- Yes, identified, capture and prosecution pending
- Yes, identified and captured, prosecution pending
- Yes, identified, captured, and prosecuted (successfully)

- Yes, identified, captured, and prosecuted (unsuccessfully)
- No, extortionist not identified, actively pursuing identification
- No, extortionist not identified, not pursuing identification
- Unsure

Q1h: Did this threat originate from someone internal or external to the organization?

- Internal  External  Unsure

Q1j: If the threat originated externally, from what geographical region did the extortion attempt originate?

(click to select)

Q2a: If your organization had a credible extortion threat made against it, would law enforcement be called to investigate?

- Yes  No  Depends on substance of threat

Q2b: If your organization had a credible extortion threat made against it, which would be first called to aid in response?

(click to select)

Q2c: If your organization had a credible extortion threat made against it, which would be second called to aid in response?

(click to select)

Q2d: If your organization had a credible extortion threat made against it, which would be third called to aid in response?

(click to select)

Q3a: Please rank the below extortion threats in terms of potential to cause serious damage to your organization (1 – Non-issue; 3 – Moderately damaging; 5 – Most damaging):

- 1 Theft and release of customer data (credit card data, purchase histories, etc.)
- 1 Theft and release of intellectual property (patents, research, etc.)
- 1 Theft and release of sensitive internal data (human resource, financial data, etc.)
- 1 Placement of illicit materials on organization computer systems
- 1 Defacement of website or other externally-facing medium
- 1 Destruction of any intellectual property, customer data, or other sensitive internal data
- 1 Denial of Service (DoS) attack or other detrimental quality of service measure
- 1 Other:

Q3b: Please rank the below concerns in terms of validity for reasons your organization may not involve law enforcement during an extortion attempt (1 – Not a valid concern; 3 – Moderate concern; Serious concern):

- 1 Loss of control over investigation
- 1 Loss of control over information systems/lengthening of business recovery
- 1 Lack of confidence in law enforcement
- 1 Fear of negative publicity
- 1 Fear of down-stream liability
- 1 Fear of retribution from extortionist
- 1 Other:

Q4a: Do you contract out (or 'offshore') any IT or IS work to non-U.S. regions, aside from help desk technicians?

- Yes  No

Q4b: Has your organization experienced any extortion attempts as a result of outsourcing to non-U.S. regions?

Yes  No

Q4c: How would you rate the cyber extortion risk potential for organizations that outsource IT and IS functions?

<u>Outsource to U.S. regions vs. non-U.S. regions</u>	<u>Outsource to non-U.S. regions</u>
<input type="checkbox"/> Greater risk	<input type="checkbox"/> Greater risk
<input type="checkbox"/> Same risk	<input type="checkbox"/> Same risk
<input type="checkbox"/> Less risk	<input type="checkbox"/> Less risk
<input type="checkbox"/> Unsure	<input type="checkbox"/> Unsure

Q5a: What do you believe is the most effective technological measure to deter cyber extortion?

Q5b: What do you believe is the most effective policy measure to deter cyber extortion?

Q6: If you feel there is more information you'd like to share with the author, including if you would like to be contacted for further discussion regarding your organization's experience with cyber extortion, please comment below: