Cyber Attacks: Prevention and Proactive Responses

VINCE FARHAT, BRIDGET McCARTHY, RICHARD RAYSMAN AND JOHN CANALE, HOLLAND & KNIGHT LLP

Search the Resource ID numbers in blue on Westlaw for more.

This Note discusses common cyber attack scenarios and sets out actions that companies can take to prevent or respond to attacks, including developing a cyber incident response plan. It also addresses the chief compliance officer's role in preventing and containing attacks and making law enforcement referrals, and civil and criminal actions companies can pursue against attackers.

Cyber attacks, including hacking, of business websites and computer systems are increasingly common. These attacks can be extremely damaging to businesses and other organizations, particularly if security is breached and confidential business and personal data compromised. Cyber attacks and the resulting security breaches are part of a rapidly expanding international cyber threat that costs companies and taxpayers billions of dollars each year in lost information and response costs. Executives face increasing pressure to prevent these attacks and must act immediately to contain any damage once an attack occurs.

This Note examines:

- The chief compliance officer's (CCO) key role in preventing and containing cyber attacks.
- Proactively developing a cyber incident response plan to report, investigate, and respond to a cyber attack.
- Common cyber attack scenarios.
- Civil and criminal legal claims that may be brought against cyber attack perpetrators.
- Recent case law relevant to some of the key issues discussed in this Note.

Cyber attacks involving personal information implicate various data privacy and security laws. For general information on US data security laws, see Practice Note, US Privacy and Data Security Law: Overview (6-501-4555). For information on state data breach notification laws, see Data Breach Notification Laws: State Q&A Tool.

WHAT IS A CYBER ATTACK?

A cyber attack is an attack initiated from a computer against a website, computer system, or individual computer (collectively, a computer) that compromises the confidentiality, integrity, or availability of the computer or information stored on it. Cyber attacks take many forms, including:

- Gaining, or attempting to gain, unauthorized access to a computer system or its data.
- Data theft, such as online exfiltration of data to an unauthorized individual or location.
- Unwanted disruption or denial of service attacks, including the take down of entire websites.
- Installation of viruses or malicious code (malware) on a computer system.
- Unauthorized use of a computer system for processing or storing data.
- Changes to the characteristics of a computer system's hardware, firmware, or software without the owner's knowledge, instruction, or consent.
- Inappropriate use of computer systems by employees, former employees, or others.

The procedures for investigating and responding to a cyber attack depend largely on the nature of the attack itself (see Common Cyber Attack Scenarios).

Regardless of the nature of a cyber attack, the CCO of a company, or an equivalent individual, must take the primary responsibility for preventing and responding to cyber attacks.

CHIEF COMPLIANCE OFFICER'S ROLE IN CYBER ATTACKS

In recent years, new and increased use of technologies such as mobile devices, social media, and cloud computing has increased the risk posed by cyber criminals. As a result, in addition to other compliance matters, for example, Securities and Exchange

Commission (SEC), Sarbanes-Oxley, and Dodd-Frank Act compliance, the CCO is now also typically responsible for:

- Deterring cyber attacks.
- Quickly containing any attacks and minimizing any financial and reputational harm.

Some companies delegate responsibility for computer systems security to their chief information officer (CIO). The CIO is usually responsible for protecting access to a company's information technology (IT) network and systems and the privacy and security of information on those systems. In some cases, the company may also have a chief privacy officer (CPO) or chief information security officer (CISO).

Whatever the company's organizational structure, the CCO must coordinate with the CIO and other company departments to prevent cyber attacks. The CCO must also work closely with the CIO, and CPO and CISO if applicable, to understand the steps being taken to deter these attacks. To some extent, the CCO operates as a chief security officer and must therefore:

- Ensure that policies and procedures for employees to follow are in place.
- Monitor the occurrence of possible cyber attacks.

Recently, in light of highly publicized cyber attacks, many companies have been elevating the CISO position. The CISO is typically a senior-level executive with a seat on the board of directors, or at least a direct line to the chief executive and board, and is responsible for:

- Assessing and managing information security risks.
- Responding to breaches and other cyber incidents.
- Establishing and implementing company security standards, policies, and procedures.
- Managing security technologies.

ACTIONS TO PREVENT OR REDUCE THE RISK OF CYBER ATTACKS

There are a number of resources a CCO may consult in developing a plan and prioritizing preventative actions, for example, the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. The Framework is a voluntary risk-based set of best practices and industry standards developed to enhance security and resilience in cyber networks (see Practice Note, The NIST Cybersecurity Framework (5-599-6825)). Generally, however, there are a number of actions that the CCO should take to prevent or reduce cyber attack risk.

Determine the Company's Security Chain

The CCO needs to determine and evaluate the company's entire security chain. If even a single link is weak, the company could be vulnerable to attack. The CCO should be cognizant of the company's role in the supply chain and communicate this role to stakeholders. Further, supply chain interdependency requires that the CCO:

- Map the existing supply chain.
- Identify and address key challenges to the supply chain, including potential security risks.
- Encourage supply chain engagement.

Develop a Compliance Work Plan

The CCO should create a written compliance plan to monitor the highest risks for a potential cyber attack. In developing this compliance plan, the CCO should start by performing a gap analysis or risk assessment. The CCO should determine the status of current cybersecurity measures and compare them to target cybersecurity measures. The compliance plan should identify steps to address the gaps between the current and target measures. The compliance plan must address cyber attack procedures in addition to other compliance matters. This should include:

- Policies and procedures.
- Codes of conduct.
- Training.
- Specific incident response procedures.

The compliance plan is a living document and should be reviewed and updated on an ongoing basis.

Prepare Legally Required Disclosures

The SEC has advised public companies that they are responsible for evaluating cybersecurity risks and disclosing these risks to investors as appropriate. CCOs of public companies therefore must assess whether their compliance plans and disclosure procedures comply with the SEC's guidance. For more information, see Standard Clause, Sample Risk Factor: Cybersecurity (9-506-9947).

Coordinate with the CIO, CPO, CISO, and Other Departments

The CCO must coordinate with the CIO, CPO, and CISO on cyber attack issues. While there is overlap of responsibilities among the CCO, CIO, CPO, and CISO roles, the CCO is responsible for coordinating efforts among all relevant corporate departments and ensuring effective communication and cooperation to prevent and respond to cyber attacks and data breaches. Key departments include:

- IT.
- Human resources.
- Legal.
- Each company business unit.

The CCO should require periodic meetings of all these departments to review policies, procedures, and coordination efforts.

Implement an Enterprise-Wide Data Risk Management Program

The CCO should, in coordination with the CIO, CPO, and CISO, implement and maintain an enterprise-wide data risk management program to mitigate risk and assure security of company and customer data.

As part of this program, the CCO should work with the IT, human resources, and other appropriate departments to restrict employee access to information. Employees should only have access to information related to their job functions.

For more information on conducting data security risk assessments, see Practice Note, Data Security Risk Assessment and Reporting (w-002-2323) and Performing Data Security Risk Assessments Checklist (w-002-7540).

Review Employee Policies

Employee policies (for example, an electronic systems use policy) should restrict employees from "unauthorized access" or "exceeding authorized access" of the company's computer systems. A policy that distinguishes between authorized employee access and unauthorized access may help companies pursue claims under the Computer Fraud and Abuse Act involving unauthorized acts by employees (for more details, see Computer Fraud and Abuse Act).

For details on developing information security policies and an example policy, see Practice Note, Developing Information Security Policies (w-001-1336) and Standard Document, Information Security Policy (w-001-2990).

Invest in Computer Security and Protection Measures

The company should invest in data security controls and procedures to deter or prevent cyber attacks. These include the most up-to-date IT protection measures, for example:

- Maintaining a current asset inventory for all computer and network hardware and software.
- Using secure configurations.
- Monitoring vulnerability reports and applying the latest security patches.
- Granting access only to those with a demonstrated business need to know.
- Protecting all passwords.
- Using read-only views of documents and materials when possible.
- Encrypting important or sensitive data and personal information.
- Using current anti-virus software and other measures to protect against malware.
- Building security into applications and systems using security-by-design principles.
- Testing mobile apps, websites, and devices to identify and address potential privacy issues and security lapses.
- Developing, implementing, and maintaining sound network security architecture and controls, such as:
  - firewalls;
  - network segmentation;
  - intrusion detection and prevention services; and
  - data loss (data leakage) prevention software.
- Monitoring and managing log files to detect security incidents.
- Monitoring activities and procedures of third-party contractors with access to the company's network and computer systems, whether direct or remote.
- Performing network scans to assess vulnerabilities.
- Monitoring activity on the network.
- Addressing common web application issues by:
  - choosing names for tables and fields that are difficult to guess;
  - housing databases, applications, and web services on separate servers; and
  - maintaining strict input validation.

For more examples of computer security and protection measures, see Common Gaps in Information Security Compliance Checklist (3-501-5491).

Adopt a Cyber Incident Response Plan and Employee Reporting Mechanisms

The company must adopt reporting mechanisms so that the CCO is promptly advised of all cyber attack incidents and can rapidly respond. All employees should be aware of the possibility of cyber attacks and where such attacks are most likely to be directed within the company (see also Cyber Incident Response Plans).

Adopt Procedures to Preserve Evidence

The CCO should ensure the company has procedures in place to secure and preserve computer-related evidence if a cyber attack occurs, to:

- Better understand and repair any damage caused by an attack.
- Aid any criminal or civil action against the violators.

Failure to properly preserve electronic evidence can adversely affect a later criminal or civil action against the violator (see also Box, Recent Case Law: Failure to Properly Secure Electronic Evidence and Practice Note, Preserving Data After a Data Breach (w-005-3417)).

Obtain Senior Management Support

The board of directors, CEO, CFO, and other senior management must support the CCO in preventing cyber attacks. This top-down approach aims to get the entire organization to support secure practices and accept compliance activities. The CCO should also have the authority to perform independent investigations when necessary.

Maintain Relationships with Law Enforcement Agencies

The CCO should create and maintain relationships with federal, state, and local law enforcement and other related regulatory agencies that deal with cyber attacks (see also Box, Reporting Cyber Crime to the Appropriate Law Enforcement Agency).

CYBER INCIDENT RESPONSE PLANS

Every company should develop a written plan (cyber incident response plan) that identifies cyber attack scenarios and sets out appropriate responses. The cyber incident response plan may be part of a global response plan. While the cyber incident response plan must be customized for each company's particular circumstances, the plan should generally address these basic components:

- Response team.
- Reporting.
- Initial response.
- Investigation.
- Recovery and follow-up.
- Public relations.
- Law enforcement.

For an example cyber incident response plan, see Standard Document, Cyber Incident Response Plan (IRP) (w-005-0419).

CYBER INCIDENT RESPONSE TEAM

The response team is responsible for developing the written cyber incident response plan and for investigating and responding to cyber attacks in accordance with that plan. Specifically, the response team, working with the CCO and other internal stakeholders as appropriate, should:

- Develop the cyber incident response plan.
- Identify and classify cyber attack scenarios.
- Determine the tools and technology used to detect and prevent attacks.
- Secure the company's computer network before any potential attack.
- Develop a checklist for handling initial investigations of cyber attacks.
- Determine the scope of an internal investigation once an attack has occurred.
- Conduct any incident investigations within the determined scope.
- Promote cybersecurity awareness within the company.
- Address data breach issues, including notification requirements.
- Conduct follow-up reviews on the effectiveness of the company's response to an actual attack.

A large e-commerce company that relies on its website for sales or other critical business operations may require a large formal response team. Smaller companies that rely less on their IT resources may have smaller and more informal teams.

DISCOVERY AND REPORTING OF CYBER INCIDENTS

The cyber incident response plan should address procedures to take on discovery and reporting of cyber attack incidents, including:

- Designating response team members to monitor industry practices to ensure that the:
  - company's information systems are appropriately updated and secured; and
  - company installs the latest software security patches to prevent or allow for early discovery of attacks.
- Continuously monitoring the company's computer and network logs to discover any incidents.
- Creating a database to track all reported incidents.
- Creating a risk rating to classify all reported incidents as low, medium, or high risk to facilitate an appropriate response.

INITIAL RESPONSE TO A CYBER ATTACK

If a potential attack is reported, the designated response team member should conduct a preliminary investigation to determine whether a cyber attack has occurred. If a cyber attack has occurred, the response team should follow the investigation checklist set out in the cyber incident response plan to conduct the initial investigation.

The initial response varies depending on the type of attack and level of seriousness. However, the response team should aim to:

- Stop the cyber attack or intrusion from spreading further into the company's computer systems.
- Appropriately document the investigation.

INVESTIGATING A CYBER ATTACK

Following the initial response assessment, the company may decide to undertake a formal internal investigation depending on the level of attack or intrusion and its impact on critical business functions. An internal investigation allows the company to:

- Gain a fuller understanding of the cyber attack or intrusion.
- Increase its chances of identifying the attacker.
- Detect previously unknown security vulnerabilities.
- Identify required improvements to computer systems.

If the company's response team or IT department lacks the capacity or expertise to conduct an internal investigation the company may wish to retain:

- Legal counsel.
- A cybersecurity consultant.

For more information on preparing for and responding to a data breach, see Practice Note, Breach Notification: Preparing for and Responding to a Data Security Breach (3-501-1474) and Data Breach Response Checklist (2-604-9645). For guidance in selecting cybersecurity consultants, see Article, Expert Q&A: Data Security Incidents—Selecting a Forensic Vendor (w-001-0405).

COMMON CYBER ATTACK SCENARIOS

Cyber attacks often fall into one or more common scenarios. Effective cyber incident response plans anticipate and prepare for these common scenarios in advance and provide preliminary investigatory questions for each scenario. Obtaining fast and accurate answers to these questions helps shape and expedite the investigation.

Some of these common cyber attack scenarios include:

- Insider attacks.
- Social engineering.
- Exploitation malware.
- Extortion and blackmail.

For help in understanding the technical issues involved in common cyber attacks, see Practice Notes:

- Cybersecurity Tech Basics: Hacking and Network Intrusions: Overview (w-003-3498).
- Cybersecurity Tech Basics: Malware and End User Attacks: Overview (w-003-4711).
- Cybersecurity Tech Basics: Ransomware: Overview (w-003-4711).

Insider Attacks

Employees or contractors may exploit their positions to hack the company's computers or otherwise compromise its IT systems. In this case, companies should immediately ask:

- What data or systems appear to be affected by the attack?
- Who is the subject of the investigation?
- What is the subject's position and tenure with the company?
- How tech-savvy is the subject?
- What is the subject's ability to harm the company?

- What kinds of digital devices does the subject typically use (for example, PC, laptop, smartphone, or other mobile devices)?
- What kinds of data and data systems does the subject have access to?
- Are audit trails available that show what systems the subject commonly accesses?
- What are the company's policies regarding digital devices and remote access to its systems?
- What are the policies regarding permissible behavior on the company's network?

Social Engineering

Social engineering is a hacking technique that uses low-tech or non-technical approaches to persuade people to compromise security procedures and disclose sensitive information. An example of this is impersonating company IT personnel and calling unsuspecting employees to get them to reveal confidential information such as computer access codes, passwords, or anti-virus software used by the company. Email is also a common means for social engineering attacks, called "phishing." These attacks may be specifically targeted at individuals who have access to sensitive or valuable information.

When social engineering is suspected, companies should immediately ask:

- Who was targeted in the attack?
- What information was potentially disclosed or breached?
- What system or data at the company was targeted?
- How was the attack discovered?
- Was the company notified by the victim or another affected party?
- Is there a reporting process in place for social engineering attacks?
- Are complete phone logs available?
- Are employees trained on how to spot, avoid interacting with, and report suspicious emails?
- What company or system weakness allowed the attack to succeed, including business processes and approval chains?

Exploitation Malware

Viruses and malware that exploit vulnerabilities in a company's computer systems are prevalent. For example, hackers may introduce them to computer systems by tricking employees into opening infected emails. Some malware is designed to steal confidential information such as Social Security numbers, credit card or bank account numbers, and bank account log in data.

Companies must have in place policies and procedures to defend against malware. Following a cyber attack, the cyber incident response plan should ensure that an investigation is done to reasonably ascertain whether any information has been stolen. The response plan should include procedures to avoid cleaning affected computer systems after a cyber attack without first performing a forensics analysis to help determine whether confidential information has been accessed or stolen.

Extortion and Blackmail

A company may receive threats from individuals claiming to have hacked its website or computer systems offering to return stolen confidential information in exchange for money or property. These extortionists frequently target small businesses because of their perceived inability to fight back. Recently, even larger organizations have fallen victim to ransomware attacks. Ransomware attacks combine malware and extortion attacks. Attackers install malware that makes a company's systems or data inaccessible, in some cases, encrypting large amounts of stored information. The attackers then demand payment to release the systems or data back to the company, often through hard-to-trace online communication and payment methods.

In these cases, the company must conduct an immediate threat assessment to determine whether its computer systems have been attacked and, if so, how it was accomplished. Companies should:

- Determine whether the extortionist's claims are real by isolating areas that may be affected to determine if and how they have been compromised and to prevent the attack from spreading.
- Determine the feasibility of restoring systems if an attack affects business critical infrastructure. This includes assessing whether restoring service will negatively affect collecting evidence in the investigation.
- Document all aspects of the investigation and secure and preserve all evidence, including logs of critical system events.

RECOVERY AND FOLLOW-UP AFTER A CYBER ATTACK

The cyber incident response plan should address the recovery of the company's computer systems by both:

- Eliminating the vulnerabilities exploited by the attacker and any other identified vulnerabilities.
- Bringing the repaired systems back online.

Once systems are restored, the response team should:

- Determine what cybersecurity management improvements are needed to prevent similar incidents from reoccurring, including increased employee training and awareness.
- Evaluate how the response team executed the response plan.
- Consider whether the cyber incident response plan can be improved.

PUBLIC ANNOUNCEMENTS AND PUBLIC RELATIONS AFTER A CYBER ATTACK

The cyber incident response plan may designate one or more executives responsible for handling press releases and other public announcements about the cyber attack including:

- The desirability of any announcements.
- The timing and content of any announcements.

The company may also have to address customer or user concerns and take measures to restore confidence and loyalty, for example, where there has been theft of credit card or other personal information or denial of service.

LAW ENFORCEMENT INVESTIGATIONS OF CYBER ATTACKS

Many security-related incidents do not result in criminal investigations because companies do not contact law enforcement. Several law enforcement agencies investigate and prosecute cyber attacks and other computer incidents (see Reporting Cyber Crime to Law Enforcement).

If the company operates in a sensitive area, it may consider reaching out to relevant law enforcement representatives before an incident occurs to discuss:

- When it should report incidents.
- How it should report incidents.
- What evidence it should collect.
- How it should collect evidence.

The cyber incident response plan should designate one incident response team member, for example, the CCO, as the primary point of contact with law enforcement.

CUSTOMIZING THE CYBER INCIDENT RESPONSE PLAN

CCOs, CIOs, CPOs, and CISOs should work closely with their IT departments, response team, legal counsel, and, where appropriate, cybersecurity consultants, to develop a cyber incident response plan that addresses the specific needs of their organization.

Helpful resources include:

- The NIST Computer Security Incident Handling Guide (Rev. 2), which assists organizations in:
  - establishing computer security incident response capabilities; and
  - handling incidents efficiently and effectively.
- The NIST Cybersecurity Framework, which guides organizations in developing their information security programs, including event detection, response, and recovery (see Practice Note, The NIST Cybersecurity Framework (5-599-6825)).
- The SANS Institute, which provides:
  - information security training and security certification; and
  - research documents about various aspects of information security.

For a form cyber incident response plan with drafting notes, see Standard Document, Cyber Incident Response Plan (IRP) (w-005-0419).

REPORTING CYBER CRIME TO LAW ENFORCEMENT

Designating a Law Enforcement Liaison

Large-scale cyber attacks should always be reported to law enforcement. Companies should designate a response team member as the primary point of contact with law enforcement, including:

- Federal investigatory agencies.
- State attorneys general and district attorneys.
- State and local law enforcement.

The designated liaison should understand the jurisdictional issues arising from the location of the company, its assets, and the attacker. For example, a company based in one state may have a server located in a second state that is attacked from a system in a third state, which is being used remotely by an attacker in a fourth state or another country. Dealing with this scenario may require the assistance of law enforcement in multiple jurisdictions.

Law Enforcement Agencies that Investigate Internet Crime

The primary federal law enforcement agencies that investigate internet crime include:

- The Federal Bureau of Investigation (FBI).
- The US Secret Service (Secret Service). US Immigration and Customs Enforcement (ICE).
- The US Postal Inspection Service.
- The Bureau of Alcohol, Tobacco, and Firearms (ATF).

Each agency has offices located in every state to which crimes may be reported. In general, suspected crimes may be reported to the local office of an appropriate law enforcement agency by a telephone call and by requesting the Duty Complaint Agent. Each federal law enforcement agency also has an office in Washington, DC, with agents who specialize in particular areas. For example, the FBI and the Secret Service both have headquarters-based specialists in computer intrusion cases.

The Department of Justice provides information on the agencies that may be appropriate for reporting different kinds of cyber crime (see Box, Reporting Cyber Crime to the Appropriate Law Enforcement Agency).

Additional Cyber Crime Resources

Another resource for reporting cyber crime is the Internet Crime Complaint Center (IC3). IC3 is a partnership between the FBI and the National White Collar Crime Center that receives, develops, and refers criminal complaints regarding cyber crime. It gives cyber crime victims a reporting mechanism that alerts authorities to suspected criminal violations.

For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving internet related crimes.

For state-related cyber questions, the National Association of Attorneys General maintains a Computer Crime Point of Contact List.

CRIMINAL PROSECUTION

Companies should consider preparing formal referrals to law enforcement for possible criminal prosecution when an internal investigation leads to evidence of the attacker's possible identity. Companies considering this course of action can retain white collar crime or intellectual property counsel to guide them through the investigation, referral, and criminal proceedings.

The outcome of a criminal prosecution may depend on the company's ability to provide evidence and testimony. Counsel should be prepared to help prosecutors present complex computer crime evidence to a judge and jury. Counsel should also evaluate civil remedies and damage claims against the attackers.

CIVIL AND CRIMINAL REMEDIES FOR CYBER ATTACKS

IDENTIFYING THE HACKERS

The viability of any criminal or civil cyber attack prosecution initially depends on the company's or law enforcement agency's ability to identify and locate the hacker. In some cases, an entire network or organization of hackers may be involved. Many hackers are located outside of the US, presenting jurisdictional issues. Many suspect that foreign governments or government-sanctioned groups initiate some attacks.

If the company has the IP addresses of the hacker, it may be able to identify the internet service provider (ISP) through which the hacker launched the attack. The company may then demand that the ISP identify the hacker. If the ISP denies this request, the company can file either:

- A John Doe or Jane Doe action against the anonymous hacker to get discovery and issue a subpoena to the relevant ISP to reveal the hacker's identity.
- If copyright infringement is involved, a subpoena action under the Digital Millennium Copyright Act (DMCA) (Pub. L. No. 105-304, 112 Stat. 2860). The DMCA authorizes copyright owners to subpoena an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity. The copyright owner can use this subpoena to request the names of alleged hackers.

However, sophisticated attackers can hide their identities by various methods, including using someone else's computer to launch an attack. This makes it difficult to identify the hacker, because multiple ISPs may be involved, each with only incomplete information. Forensic consulting firms can assist with this process of identification, but it is time consuming, expensive, and not always successful. Companies may elect to pursue hackers on a selective basis and publicize successful results to send a deterrent message. Companies may also contact law enforcement for assistance (see Reporting Cyber Crime to Law Enforcement).

COMPUTER FRAUD AND ABUSE ACT

The Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030) is the main federal criminal statute regulating hacking and other computer crimes. The CFAA generally criminalizes:

- Accessing computers without, or in excess of, authorization.
- Using unlawfully accessed computers to obtain information that defrauds or causes loss or damage to another or the US government.

Protected Computers under the CFAA

The CFAA governs cases involving protected computers, which are defined as computers that meet one or more of the following criteria:

- Exclusively used by a financial institution or the US government.
- Not covered by the above, but:
  - that are used by or for a financial institution or the US government; and
  - where the offense affects the computers' use by or for a financial institution or the US government.
- Used in or affecting interstate or foreign commerce or communication. This includes use of computers located outside the US that affects:
  - interstate or foreign commerce; or
  - communication within the US.

Prohibited Acts under the CFAA

The CFAA prohibits:

- Computer trespassing (for example, hacking) in a government computer.
- Computer trespassing that exposes certain governmental, credit, financial, or computer-housed information.
- Damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce. Examples of this type of damage include:
  - a worm;
  - a computer virus;
  - a trojan horse;
  - a time bomb;
  - denial of service attack;
  - other forms of malware or cyber attacks; and
  - cyber crime or cyber terrorism.
- Committing fraud that involves unauthorized access to a protected computer.
- Threatening to damage a protected computer.
- Trafficking in passwords for a government computer or password trafficking that affects interstate or foreign commerce.
- Accessing a computer to commit espionage.

It is also a crime to attempt or conspire to commit any of these acts.

Penalties under the CFAA

The penalties for committing CFAA offenses range between:

- Imprisonment for up to one year for simple cyber trespassing.
- A maximum of life imprisonment when death results from intentional computer damage.

The Computer Abuse Amendments Act of 1994 added civil remedies to the CFAA allowing any person who suffers damage or loss through a CFAA violation to maintain a civil action against the violator for:

- Compensatory damages.
- Injunctive or other equitable relief.

(18 U.S.C. § 1030(g).)

In particular, the CFAA authorizes a civil action against a person who knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorization. The plaintiff generally must allege losses of $5,000 or more.

OTHER CIVIL AND CRIMINAL REMEDIES

Other civil and criminal remedies may be available to cyber attack victims, depending on the circumstances, under:

- The Wiretap Act and Electronic Communications Privacy Act (ECPA) (see Wiretap Act and ECPA).
- The Stored Communications Act (SCA) (see SCA).
- Trade secrets law (see Trade Secret Theft).
- Copyright and trademark infringement actions (see Copyright and Trademark Infringement).
- The DMCA (see DMCA Anti-Circumvention).
- The Racketeer Influenced and Corrupt Organizations (RICO) Act (see RICO Act).
- State-level computer crime laws (see State Computer Crime Laws).
- Other civil actions (see Other Civil Actions).

Companies can also refer criminal cyber attacks to the appropriate law enforcement authorities for prosecution (see Reporting Cyber Crime to Law Enforcement).

Wiretap Act and ECPA

The Wiretap Act, as amended by the ECPA:

- Prohibits the interception, use, or disclosure of wire and electronic communications unless a statutory exception applies.
- Authorizes civil actions by private persons.

Violators are subject to a range of sanctions, including:

- Actual damages.
- Punitive damages.
- Statutory damages (the greater of $10,000 or $100 a day per violation).
- Attorneys' fees.

(18 U.S.C. §§ 2510-2522.)

SCA

The SCA makes it illegal to intentionally access, without or in excess of authorization, a facility through which an electronic communication service is provided to obtain or prevent authorized access to a wire or electronic communication while it is in storage in the facility.

Offenses are punishable by fine, imprisonment, or both.

A civil action may be commenced by any:

- Electronic communications services provider.
- Subscriber.
- Other person aggrieved by a violation of the law.

Civil damages may include:

- Actual damages.
- The violator's profits.
- Punitive damages.
- Costs.
- Attorneys' fees.

(18 U.S.C. § 2701-2712.)

Trade Secret Theft

Where trade secret theft is involved, cyber attack victims may commence a civil action under the relevant state trade secret act or common law. The Defend Trade Secrets Act of 2016 (DTSA) also creates a federal private cause of action for trade secret misappropriation. The DTSA supplements but does not preempt state law.

For more information on trade secrets generally, see Practice Note, Protection of Employers' Trade Secrets and Confidential Information (5-501-1473) and for state-specific information, see Trade Secret Laws: State Q&A Tool.

Copyright and Trademark Infringement

Civil actions may be available for copyright infringement under the federal Copyright Act and trademark infringement under the federal Lanham Act or state trademark law.

The Copyright Act also provides criminal penalties for copyright infringement (17 U.S.C. § 506). The law penalizes willful infringement of a copyright for commercial advantage or private financial gain, among other activities. Violations are punishable by imprisonment, fine, or both (18 U.S.C. § 2319).

For more information on copyright and trademark law, see Practice Notes, Copyright Infringement Claims, Remedies, and Defenses (3-517-6950) and Trademark Infringement and Dilution Claims, Remedies, and Defenses (1-508-1019).

DMCA Anti-Circumvention

The DMCA prohibits the:

- Circumvention of technological, anti-piracy measures built into most commercial software to control access to copyrighted works.
- Manufacture, sale, or distribution of code-cracking devices used to illegally copy software.

The law authorizes civil actions for:

- Actual or statutory damages.
- Injunctive and other equitable relief.
- Attorneys' fees.

(17 U.S.C. § 1201.)

RICO Act

The RICO Act provides criminal penalties, including up to 20 years imprisonment, for acts performed as part of an ongoing criminal organization. Specifically, the RICO Act penalizes those engaged in a pattern of racketeering activity, which includes at least two acts of fraud and related activity in connection with:

- Identification documents.
- Wire fraud.
- Criminal infringement of a copyright.
- Trafficking in counterfeit labels.

The RICO Act also provides for a civil action by any person injured in his business or property, through a RICO Act violation, for:

- Recovery of money damages, including treble damages.
- Costs.
- Reasonable attorneys' fees.

(18 U.S.C. §§ 1961-1968.)

State Computer Crime Laws

Criminal and civil actions may be brought under various state laws targeting computer fraud. For example, in California it is illegal to knowingly access and without permission alter, damage, delete, destroy, or otherwise use any data, computer, computer system, or computer network to:

- Defraud.
- Deceive.
- Extort.
- Wrongfully control or obtain money, property, or data.

Other prohibited activities include knowingly:

- Accessing and copying data from a computer or computer system or network.
- Using without authorization, disrupting, or denying a computer service.
- Introducing contaminants into a computer service.

Also, the owner of a computer system or program who suffers damage or loss through a violation of the law may bring a civil action for:

- Damages.
- Injunctive or other equitable relief.
- Attorneys' fees.

(Cal. Penal Code § 502.)

State laws may also authorize civil actions against the parents of a minor hacker.

Other Civil Actions

Civil actions may also be available for:

- Violating the terms and conditions of use of a company's website, including:
  - contract-based liability; and
  - common law and statutory liability.
- Computer trespass and conversion.

OTHER ACTIONS TO DETER OR MITIGATE CYBER ATTACKS

In addition to pursuing available civil and criminal claims, companies should consider other options to respond to cyber attacks and mitigate any resulting losses, including:

- Cease and desist letters (see Cease and Desist Letters).
- DMCA takedown notices (see DMCA Takedown Notices).
- Cyber liability insurance coverage (see Cyber Liability Insurance Coverage).

CEASE AND DESIST LETTERS

When there are ongoing violations, a company may decide to issue a cease and desist letter to a hacker before commencing a civil action. The letter should:

- Aim to persuade the hacker to cease violations under the threat of civil actions and remedies.
- If appropriate, inform the hacker that **if** the alleged conduct rises to the level of a criminal violation, and a case is brought by the proper authorities, the hacker could be subject to criminal penalties.

However, the letter should **not** directly accuse the hacker of criminal conduct or threaten criminal prosecution.

Before deciding to issue a cease and desist letter, the company should evaluate the possible responses from the hacker, which may include:

- Disregarding the letter completely.
- Posting it on a website in an effort to ridicule enforcement efforts.
- Adopting alternative hacking approaches.
- Terminating violations.

DMCA TAKEDOWN NOTICES

Hackers may post materials on third-party websites or their own websites that infringe copyright. ISPs seeking the DMCA safe harbor for infringing acts by their third-party users must remove copyright infringing material from users' websites on notice. A copyright owner can contact the ISP or website operator (together, service providers) of the infringing website through a DMCA takedown notice to request that the service providers:

- Remove or disable access to the infringing material or activity.
- Cease linking or referring users to other online locations that contain infringing material or activity.

The DMCA takedown notice should be sent to the appropriate service and:

- Explain the infringements appearing on the site.
- Request that the site:
  - be shut down; or
  - remove any infringements.

For the DMCA notice to be effective, it must comply with certain statutory requirements. For a sample DMCA takedown notice, see Standard Document, DMCA Complaint (Takedown Notice) (3-502-6258).

If the service provider seeks safe harbor protection, it must remove the infringing material or disable access to it in response to a DMCA notice that substantially complies with statutory requirements. If a service provider disregards a proper DMCA takedown notice, it may be held responsible for the infringements in any lawsuit.

The DMCA allows the alleged infringer to issue a counter-notice in response to a DMCA takedown notice. The service provider must forward the counter-notice to the copyright owner. If the alleged infringer issues a counter-notice, the service provider must restore access to the infringing site or materials if the copyright owner does not sue the alleged infringer within ten days after it receives the counter-notice. When sending a counter-notice, the alleged infringer must:

- Provide its name and address.
- Submit to federal court jurisdiction.

This may help the copyright owner maintain a lawsuit with less concern for jurisdictional and certain other defenses.

CYBER LIABILITY INSURANCE COVERAGE

Companies should carefully review their liability insurance policies and consult with their insurance brokers to determine whether they are adequately insured for cyber attack losses. Companies may want to obtain insurance coverage for:

- Privacy and data breach liability.
- Computer hardware, software, and data damage or loss.
- Crisis management.
- Business interruption, denial of service attack, and lost income.
- Loss of business reputation.
- Cyber extortion.
- Media or web content liability.

For detailed information on cyber insurance, including considerations in selecting and applying for coverage, see Practice Note, Cyber Insurance: Insuring for Data Breach Risk (3-502-6258).

RECENT CASE LAW

Representative cases discussing various civil and criminal legal issues arising in cyber attacks are described below.

DATA BREACH LITIGATION

Recently, plaintiffs have filed lawsuits based on cyber breaches against large national and multi-national companies, putting companies on notice about potential liability for breaches and raising public awareness of the issue. Three notable cases include lawsuits filed against Target Corporation, Yahoo! Inc., and Wyndham Worldwide Corporation, which highlight the importance of instituting appropriate and aggressive security measures and signal a wave of potential future litigation.

Target Corporation

In November and December 2013, Target Corporation suffered a data breach that compromised the personal information of up to 110 million people. Class action plaintiffs filed lawsuits in various federal district courts throughout the country, which were consolidated in front of a US district court judge in Minnesota (*In Re: Target Corp. Customer Data Security Breach Litig.*, No. 14-2522 (D. Minn. filed Apr. 2, 2014)). In December 2014, the court issued a decision denying Target's motion to dismiss. In November 2015, the court approved a $10 million settlement that also required Target to improve its data security practices in significant ways (see Legal Update, Target's $10 Million Data Breach Settlement Gets Final Approval: D. Minn. (w-000-8890)).

Yahoo! Inc.

Yahoo! Inc. suffered two separate data breaches in 2013 and 2014 that compromised the personal information of over 500 million accounts. Plaintiffs filed class action lawsuits in late 2016 that were consolidated in the Northern District of California in February of 2017 (*In Re: Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-MD-02752-LHK (N.D. Cal. filed Dec. 07, 2016)). A consolidated complaint was filed on April 12, 2017.

Wyndham Worldwide Corporation

Another important lawsuit for companies to note is *Federal Trade Commission v. Wyndham Worldwide Corp., et al.*, No. 13-1887 (D.N.J. filed Mar. 26, 2013). The FTC sued Wyndham Worldwide Corporation and its subsidiaries in 2012 after an alleged theft of consumer credit and debit card information occurring between April 2008 and January 2010. The FTC alleged that Wyndham failed to employ reasonable and appropriate data security measures to protect consumer information from theft. These alleged security inadequacies included incorrectly configured software, insecure computer servers, and insufficient (weak) passwords. Wyndham filed a motion to dismiss, and on April 7, 2014, the US District Court for the District of New Jersey issued an opinion denying Wyndham's motion (10 F.Supp.3d 602 (D.N.J. 2014)). The court:

- Rejected Wyndham's argument that the FTC must issue regulations before bringing an unfairness claim under the FTC Act.
- Refused to carve out a data security exception to the FTC's authority.

While upholding the FTC's authority over data security, the court noted that the ruling did not give the FTC a blank check to prosecute lawsuits against every company that experiences a cyber breach.

The US Court of Appeals for the Third Circuit upheld the district court ruling and rejected Wyndham's arguments. Notably, in response to Wyndham's argument that the FTC had failed to provide fair notice of what data security practices might state a claim, the court pointed to the FTC's publication, Protecting Personal Information: A Guide for Business, and the FTC's data security complaints and consent decrees as providing notice to regulated parties of the FTC's standards (*FTC v. Wyndham Worldwide Corp*, 799 F.3d 236, 256 (3d Cir. 2015)). For more information on the FTC's data security standards, see Practice Note, FTC Data Security Standards and Enforcement (8-617-7036).

In December 2015, the FTC announced a settlement with Wyndham. Under the 20-year agreement's terms, Wyndham must, among other things:

- Establish, implement, and maintain a comprehensive information security program to protect the security, confidentiality, and integrity of customers' payment card data.
- Annually obtain an independent, third-party written assessment of its information security program that demonstrates compliance with the Payment Card Industry (PCI) Data Security Standards (DSS), or a comparable FTC-approved standard. For more information on the PCI DSS, see Practice Note, PCI DSS Compliance (8-608-7192).
- In the event of a data breach affecting more than 10,000 payment card numbers, obtain an independently produced PCI Forensic Investigator Final Incident Report, or a comparable FTC-approved report, within 180 days of the breach's discovery.
- Provide the FTC with copies of all such assessments and reports within ten days of receiving them from its independent assessors or investigators.

IMMEDIATE DISCOVERY OF HACKER IDENTITIES

In *Liberty Media Holdings, LLC v. Does 1-59*, a California district court allowed a website owner to conduct immediate discovery against unknown defendants who allegedly unlawfully bypassed the website's protective payment and login procedures, and accessed copyrighted materials (97 U.S.P.Q. 2d 1986 (S.D. Cal. 2011)).

The website owner provided the unique IP addresses assigned to each defendant and the court found that the owner sufficiently alleged:

- Unauthorized access by the defendants under the CFAA.
- Intentional access to stored electronic data in violation of ECPA.
- Unauthorized reproduction and distribution of the plaintiff's copyrighted works on local hard drives in violation of the Copyright Act.

The court allowed the website owner to serve subpoenas on the defendants' ISPs for information sufficient to identify the unknown parties attached to the IP addresses.

FAILURE TO PROPERLY SECURE ELECTRONIC EVIDENCE

In *United States v. Koo*, an Oregon federal district court held that an image of the hard drive from an employee's company-issued laptop was inadmissible to prove the contents of the computer at the time it was confiscated because of evidence that before handing over the laptop to the FBI for processing, a supervisor:

- Booted the machine.
- Accessed files.
- Allegedly altered content.

(770 F. Supp. 2d 1115 (D. Or. 2011).)

The defendants, former employees of the complainant, were charged with wire fraud, trade secret theft, and computer fraud, among other things, arising out of their alleged copying of confidential company data to start a competing enterprise. The court granted the defendants' motion to exclude two hard drive images the FBI took of the defendant's laptop for failure to authenticate them under Rule 901 of the Federal Rules of Evidence.

The court found that the government could not make a prima facie showing that the laptop image was in substantially the same condition as the laptop seized from the defendant.

DETERMINING VALUE UNDER THE CFAA

In *United States v. Batti*, the US Court of Appeals for the Sixth Circuit affirmed the district court's decision finding that a felony conviction under the CFAA on the basis that the value of electronic information wrongfully obtained exceeded $5,000 (18 U.S.C. 1030(2)(B)(iii)), does not require that the:

- Unauthorized access cause loss.
- Defendant profit from his intrusion.

(631 F.3d 371 (6th Cir. 2011).)

The Sixth Circuit affirmed the defendant's felony conviction under the CFAA for improperly accessing confidential files from his employer's computer servers, rejecting the defendant's argument that the value of the proprietary television commercial footage wrongfully obtained did not exceed the $5,000 statutory requirement. Because no readily ascertainable market value for the corporate advertising footage existed, a trier of fact need only determine the value of the information through some appropriate means. The Sixth Circuit determined that the cost of production of that footage was a permissible basis on which to rely in determining whether the value of the information obtained exceeded $5,000.

The Sixth Circuit also affirmed that the lower court's restitution award for the company's expenses for IT security company services and legal advice of $47,565 was not excessive.

EXPLORING THE CFAA'S REACH

In *United States v. Nosal*, the US Court of Appeals for the Ninth Circuit held that a former employee's directing others to use a current employee's login to access a prior employer's system violated the CFAA's prohibition on accessing a protected computer without authorization (828 F.3d 865 (9th Cir. 2016), *amended by* 844 F.3d 1024 (9th Cir. 2016)).

The Ninth Circuit continues to explore the CFAA's boundaries. In *Facebook, Inc. v. Power Ventures, Inc.*, the court held that a commercial entity was liable under the CFAA when it accessed a public website after the website owner explicitly revoked permission in a cease and desist letter. However, the court also noted that violating a website's terms of use, without more, is not sufficient to create CFAA liability (828 F.3d 1068 (9th Cir. 2016), *amended and superseded by* 844 F.3d 1058 (9th Cir. 2016)).

REASONABLENESS OF BANK SECURITY PROCEDURES AGAINST CYBER ATTACKS

In *Patco Construction Co. v. People's United Bank*, unknown hackers initiated unauthorized automated clearing house (ACH) wire transfers from the plaintiff's commercial bank account. The plaintiff brought claims against the bank for recoupment of the funds. The district court found that the bank's security procedures were commercially reasonable under Article 4A of the UCC and complied with Federal Financial Institutions Examination Council guidelines. This was because the security features (including company IDs and passwords, individual user IDs and passwords, and challenge questions and answers) provided multilayered security (No. 09-503, 2011 WL 3420588 (D. Me. Aug. 4, 2011)).

However, the US Court of Appeals for the First Circuit disagreed, focusing on the bank's decision to trigger challenge questions for any transaction over $1, which increased the frequency with which a user was required to enter the answers and therefore increased the security risks presented by keyloggers and other malware. In light of the increased risk, the court found that the bank's failure to monitor and immediately notify the customer of abnormal transactions flagged by the bank's security systems was not commercially reasonable. The court found the failure to add additional procedures especially unreasonable in light of the bank's knowledge of ongoing fraud. (684 F.3d 197 (1st Cir. 2012).)

In another case involving fraudulent wire transfers, the US District Court for the Eastern District of Michigan found that a bank failed to show that it shut down fraudulent wire transfer activity in the customer's account within a reasonable time after receiving an alert of suspicious activity (*Experi-Metal v. Comerica Bank*, No. 09-14890, 2011 WL 2433383 (E.D. Mich.

June 13, 2011)). The court determined that the bank did not act promptly enough to stop fraudulent wire transfers in light of, among other things:

- The volume and frequency of the payment orders, which included many transfers within hours.
- The $5 million overdraft created by the fraudulent wire transfers in what was regularly a zero balance account.
- The customer's limited prior wire transfer activity.
- The destinations and beneficiaries of the funds, which included individual accounts in Russia and Estonia.
- The bank's knowledge of previous and current phishing schemes against accountholders.

Bank customers share online security responsibilities. In *Choice Escrow and Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611 (8th Cir. 2014), the US Court of Appeals for the Eighth Circuit refused to hold the bank liable for $440,000 stolen from Choice Escrow's account in a fraudulent online wire transfer. The bank used several security measures to protect wire transfers, including:

- Unique user identifiers and password controls for its online banking software.
- Daily transfer limits.
- Device authentication that limited users to accessing accounts through known devices or answering additional challenge questions for access through unknown devices.
- Dual control that required using two separate online banking accounts to create and approve a particular transfer.

In affirming the district court's ruling that Choice Escrow should bear the loss of funds, the Eighth Circuit held that the bank's security measures were commercially reasonable. The court emphasized Choice Escrow's refusal to use dual control, despite the added protection against attacks just like the one Choice Escrow experienced and the apparent ease in implementing it.

AUTO-FORWARDING ANOTHER PARTY'S EMAILS PROHIBITED BY WIRETAP ACT

In *United States v. Szymuskiewicz*, the US Court of Appeals for the Seventh Circuit held that automatic forwarding of an employee's emails by another employee was an intentional interception of electronic communications in violation of the federal Wiretap Act (622 F.3d 701 (7th Cir. 2010)).

The court rejected the defendant's argument that:

- Setting up an auto-forwarding rule in Microsoft Outlook was not an interception of the emails while they were in transit.
- At most, the defendant could only be convicted of violating the SCA (see SCA), which prohibits accessing electronic data in storage.

The court found that the interception was contemporaneous with the communication because:

- Either the company's regional server or the supervisor's computer made copies of the messages for the defendant within a second of each message's arrival.
- Evidence showed that the Outlook rule was implemented on the server side, which was normal for Outlook, and such copying was an unlawful interception.

The court concluded that under the Wiretap Act, an intentional interception is enough and a prosecutor does not have to show that the intruder obtained valuable information through the interception.

For more information, see Wiretap Act and ECPA and SCA.

REPORTING CYBER CRIME TO THE APPROPRIATE LAW ENFORCEMENT AGENCY

Type of Cyber Crime	Investigative Law Enforcement Agency
Computer intrusion (for example, hacking)	■ FBI local office ■ Secret Service ■ Local police department
Password trafficking	FBI local office
Internet fraud matters that have a postal mail nexus	US Postal Inspection Service
Internet fraud and SPAM	■ FBI local office ■ Secret Service (Financial Crimes Division) ■ Federal Trade Commission (online complaint) ■ Securities and Exchange Commission (online complaint for investment fraud-related SPAM)
Internet harassment and bomb threats	■ FBI local office ■ ATF local office