# THE US-ISRAEL LEGAL REVIEW 2021

# Startups, Unicorns and the 'SPAC' Phenomenon

GLOBAL LEGAL MEDIA
STRATEGIC LAW FIRM MARKETING

A GLOBAL LEGAL MEDIA & NISHLIS LEGAL MARKETING PUBLICATION

NISHLIS LEGAL MARKETING SETTING THE BENCHMARK

IN ASSOCIATION WITH:
ACC Association of Corporate Counsel ISRAEL

CARTER/LEDYARD

# Ransomware Attacks: What You Should Know if You Do Business in the United States

*This article explores various U.S. government responses to the growing danger of cybersecurity breaches, and provides Israeli companies with legal and practical considerations for dealing with the threat of ransomware attacks.*

Companies and governmental authorities worldwide have been grappling with the growth of cybersecurity attacks over the past several years, and ransomware attacks have been particularly on the rise. Ransomware is a type of malware deployed by hackers who threaten to publish the victim's data or perpetually block access to its systems unless a ransom is paid. The U.S. government reported a 21% increase in ransomware attacks and a 225% increase in ransomware-related losses from 2019 to 2020. Ransomware criminals do not discriminate—with attacks being carried out against small companies, non-profits and charities, government agencies, school districts, hospitals, critical infrastructure facilities such as pipelines, as well as large global companies in key industries. The average ransom demand in the first half of 2021 was reportedly up to $570,000 from an average of $312,000 in 2020. In two high profile cases in the past year, Colonial Pipeline paid a ransom of $5 million and JBS SA, the world's largest meat supplier, paid an $11 million ransom. The ransom costs are typically only a small fraction of the total costs to organizations from such attacks.

Israel has a rich history of cybersecurity knowledge, and Israeli cybersecurity companies are currently at the forefront of the industry. Many of the founders of the leading Israeli cybersecurity companies have previously served in the Israel Defense Forces' Unit 8200 (the equivalent of the NSA) or in related units. Notwithstanding the depth of Israeli cybersecurity experience, Israel and Israeli companies are victimized by cybersecurity and ransomware attacks on a consistent basis. In particular, Israeli governmental entities have experienced a significant increase in the number of attacks carried out by hostile elements, including Iran and its affiliates, seeking to disrupt or access Israel's national infrastructure IT systems. In October 2021, the Hillel Yaffe Medical Center in Hadera, Israel was the victim of a highly-publicized ransomware attack.

This article will explore various U.S. government responses to the growing cybersecurity threats, and provide legal and practical considerations for properly preparing for and responding to the threat of ransomware attacks for Israeli companies doing business in, or with any nexus to, the U.S. As the Mishnah says, *"he who foresees events to come is truly wise."*

## I. HOW THE U.S. GOVERNMENT IS RESPONDING TO RANSOMWARE ATTACKS

In May 2021, a Russian hacker gang calling itself "DarkSide" inserted malware that froze the

operating systems of the Colonial Pipeline; the hackers demanded a very large ransom in Bitcoin to disable the malware. Colonial paid a ransom of almost $5 million in order to restart operations, but its pipeline service was disrupted for days, resulting in shortages, panic buying and gas hording at the pump, and significant gas price increases for customers along the route of the Colonial pipeline between Houston, Texas and New York City. While Colonial, aided by software security firms and government experts, was able to resume operations, it incurred significant financial costs and losses as well as damage to its reputation and consumer confidence. It also broadly affected businesses and governmental operations in the United States.

In the wake of this well-publicized attack, on May 12, President Biden issued an Executive Order in an effort to improve cyber security at federal government agencies and at private companies that supply software and other goods and services to the government. The Executive Order required the following immediate initiatives:

- Increased sharing of information about cyber threats and risks amongst service providers and federal agencies in order to accelerate incident deterrence, prevention, and response efforts.
- Standardization of procurement contract language across federal agencies to require service providers to keep records in a standardized format about cyber events, detection and responses to those events, and investigation thereof, to require providers to share that information, and to require that providers collaborate with each other and with federal agencies in cyber breach cases.
- Federal agency adoption of several security measures including using cloud technology to prevent, detect and assess and remediate cybersecurity incidents, multifactor authentication, and encryption to protect data at rest or during transmission.
- Federal agency evaluation of the security practices of software and IT service providers and requiring service providers to attest to compliance with cybersecurity best practices. Federal use of software and services that don't conform will be discontinued.
- Standardization of the federal government's playbook for responding to cybersecurity risks and incidents while also allowing for necessary flexibility to deal with different incidents as they arise. Several agencies were required to collaborate with private sector players.
- Standardization of the logging of cyber incidents, with rules governing encryption and retention of logs.
- Early detection of cybersecurity vulnerabilities and incidents on federal agency networks.
- Establishment of a Cyber Safety Review Board, comprised of federal officials and representatives from private-sector entities.
- The National Institute of Standards and Technology ("NIST") was directed to publish security ratings for commercially available software. In November 2021, NIST released draft criteria for a cybersecurity labeling system focused on consumer software. Released for public comment, the proposals set out baseline security standards that vendors would have to meet to earn certification.

Companies that do business with the U.S. government should immediately assess, with the help of U.S. counsel, how these mandated practices and requirements affect them. Further, some of these mandates for government agencies will likely be adopted as best practices in the private sector, such as the "seal of approval" that agencies will grant to software and IT services that are accepted for government procurement, and standards

MATTHEW DUNN
PARTNER

GUY BEN-AMI
PARTNER

for incident logging and response. Insurance companies, for example, may consider whether customers adopted those steps before honoring claims for hacking incidents. Thus, the private sector should monitor these initiatives.

In addition, private sector businesses should be taking steps to respond to this heightened cyber threat environment, such as the following:

## OFAC may take enforcement action against those ransomware victims that pay ransoms

- Review cybersecurity processes and procedures in-house and with security experts. This review should include consideration of the steps that the Executive Order addresses: multifactor authentication, protocols for access to data, using cloud technology as a security tool, encryption, and a comprehensive review of cyber security safeguards and procedures, including installation of all software upgrades and patches and reviews of cybersecurity practices of service providers.
- Review cybersecurity insurance coverage. It is likely that carriers will tighten their coverage requirements as claims increase.
- Employee training. Employees and service providers are often the weakest link in cybersecurity, inadvertently granting access to bad actors who are phishing and spoofing. Personnel training should be refreshed on an urgent basis.

### II. RISKS OF PAYING RANSOMS OR FACILITATING RANSOM PAYMENTS

For companies doing business in the U.S., beware of paying ransoms. On September 21, 2021, the U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC") issued an Updated Advisory reminding and clarifying that it may seek sanctions against those who facilitate ransomware attacks, as well as those who make or facilitate ransom payments to cyber criminals and malicious cyber actors that OFAC has designated under its cyber-related sanctions program and other sanctions programs.

OFAC has designated several cyber entities under its cyber-related sanctions program and other sanctions programs, including its Specially Designated Nationals and Blocked Persons List. OFAC has designated foreign criminal organizations known to have perpetrated cyberattacks, as well as entities that support and facilitate such attacks. U.S. persons are generally prohibited from engaging in or facilitating transactions with entities and individuals that have been designated on OFAC sanctions lists or those located in embargoed and sanctioned countries and regions (such as Cuba, Iran, North Korea, and the Crimea region of Ukraine).

While the U.S. government and its law enforcement agencies have openly discouraged the payment of ransoms to ransomware criminals, the government now warns that it may impose civil penalties based on strict liability if such payments are made to an entity or person designated under one of its sanctions programs. OFAC may take enforcement action against those ransomware victims that pay ransoms to listed persons or entities and against those that facilitate such payments, including cyber insurance providers, cybersecurity forensics and incident response firms, and financial services firms that process ransom payments. OFAC indicates that this aggressive step is warranted because ransom payment proceeds are often used to fund other criminal activity and activities that threaten national security and U.S. foreign policy. Such ransom payments incentivize additional ransomware attacks, and the payments do not guarantee that the criminals will restore access to lost or frozen data or prevent further attacks.

As a way to avoid or mitigate the risk of ransomware attacks, OFAC suggests that entities do the following:

- Implement a risk-based sanctions compliance program with procedures to minimize and avoid transactions with entities or individuals on sanctions lists.
- Implement a robust cybersecurity compliance program, which includes cybersecurity training, incident response plans, authentication protocols, and antivirus and anti-malware

software.

- Self-report ransomware attacks as soon as possible to law enforcement and other appropriate U.S. government agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) and Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP). The contact information for the relevant federal agencies is included in the Updated Advisory.
- Cooperate fully with law enforcement and other government agencies, sharing all relevant information.
- If a ransom payment to a sanctioned entity is contemplated, apply to OFAC for a license to engage in a transaction that otherwise would be prohibited.

OFAC indicates in its Updated Advisory that these actions will be considered mitigating factors in deciding on any enforcement action, while also increasing the likelihood of recovering data that was lost or frozen, holding cyber criminals accountable, and preventing future attacks.

OFAC and the U.S. government are serious about curbing ransomware attacks and will take action against those entities and individuals that facilitate such attacks. Financial institutions, virtual exchanges, and other entities involved in processing or receiving ransomware payments should have a sanctions compliance program which includes procedures to assess how their services are being used, and by what entities, in order to ensure that they are not involved in facilitating ransomware payment transactions. Entities should implement effective customer due diligence (CDD) and know your customer (KYC) processes and procedures.

Ransomware victims (including sophisticated corporations) may decide that paying ransoms is necessary or advisable to avoid the costs and burdens of business disruptions associated with a ransomware attack. However, victims of ransomware attacks and those that advise victims on such payments, including insurance companies and cybersecurity forensics and incident response firms, should ensure that ransom payments are not being made to entities or individuals that are designated on the OFAC lists. This can be checked on OFAC's website.

In addition, the U.S. government encourages victims of ransomware attacks to self-report attacks in a timely manner to, and cooperate fully with, applicable government agencies and law enforcement. Victims should consider whether they should disclose ransomware attacks to the public and whether there are any data breach reporting obligations. All entities should implement a comprehensive cybersecurity program designed to prevent cyberattacks and mitigate damage from such attacks. This program should involve training and procedural and technological safeguards.

## III. SEC CYBER-RELATED DISCLOSURE REQUIREMENTS

Many Israeli issuers whose securities are traded on U.S. exchanges such as the NYSE or NASDAQ may wonder how to comply with disclosure requirements relating to cybersecurity preparedness and the occurrence of incidents and attacks. Issuers should make sure their disclosures are accurate, tailored to the specific threat and continuously updated.

On June 11, 2021, the U.S. Securities and Exchange Commission ("SEC") announced that it would focus on cybersecurity disclosures made by public companies as part of its regulatory agenda, and it may issue a final rule soon. While there is not yet a standard language requirement for cyber-related disclosures, SEC enforcement actions over the last few years have served to provide insight on what the SEC requires and what is insufficient. The following are some lessons learned:

- Issuers must consider both the occurrence of *prior* cybersecurity incidents, including their severity and frequency, and the probability of occurrence and potential magnitude and cost (including insurance costs, if applicable) of future cybersecurity incidents.
- It can be very problematic to describe cybersecurity and data privacy breaches as hypothetical risks in SEC filings or to the media if an issuer has already experienced an incident.
- Reportable events are not limited to breaches or attacks. An exposed vulnerability alone can trigger the requirement for disclosure even if there is no evidence that third parties actually accessed any information.
- Issuers should establish policies and procedures

to ensure their internal controls are efficient and that information about cybersecurity risks and incidents is communicated to the appropriate disclosure personnel.

## IV. STATE CYBER AND DATA PRIVACY LAWS

While the U.S. does not have a federal cybersecurity or data protection law, several U.S. states have laws and regulations that require companies doing business in such states and/or which collect personal data of its residents to, among other things, institute data protection and security programs and safeguards and notify various parties of certain cyber incidents. In many cases, the monetary penalties for violations can be severe. Notification may be required to applicable regulators, law enforcement, or other authorities, as well as to affected individuals. If an applicable breach of personal information occurs, companies may have to prepare and distribute notifications to affected individuals.

**Reportable events are not limited to attacks. An exposed vulnerability alone can trigger the requirement for disclosure**

In addition, a few states have enacted data privacy laws which, like the EU's General Data Protection Regulation ("GDPR"), provide consumers with certain rights with respect to their personal data and place significant obligations on entities that collect such data. As with the GDPR, there can be potentially significant penalties for violations. Many other states have proposed such legislation thus it is important to monitor developments in this area.

For Israeli-affiliated companies doing business in the U.S., it is important to assess which state laws may apply. For example, businesses that collect personal data of New Yorkers might be subject to New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act. The SHIELD Act was passed in July 2019, amending the existing data breach notification law and imposing more stringent data security requirements on companies which collect information on New York residents. It requires that covered entities have sufficient administrative, technical, and physical safeguards in place and imposes reporting requirements on these entities when there has been a data breach. While New York has not yet passed a comprehensive GDPR-like data privacy law (such as those in California, Virginia, and Colorado), a proposed New York law is in the legislative process.

## V RANSOMWARE ATTACKS: IMMEDIATE STEPS AND BEST PRACTICES

While individual circumstances of a ransomware attack will dictate the proper response, the following are some general tips and best practices:

- follow your internal Incident Response Plan (draft such a plan if you don't have one).
- secure the IT systems.
- limit communication to and from the impacted systems and do not commit any action which might erase clues, contaminate evidence, or otherwise inadvertently aid the attacker.
- conduct an initial investigation of what happened and the cause, what information was accessed, what systems were compromised, and which accounts may have been utilized.
- notify management and communicate with firm employees and/or clients (as necessary) on a regular basis about the status of the incident.
- consider contacting law enforcement.
- report incident to your insurance provider to ascertain whether preferred cyber service providers are required and to assess the scope of insurance coverage. In some cases, policies will cover costs associated with breach response, including mitigation/recovery expenses, extortion/ransom payments, investigation expenses, and crisis response expenses, reporting/notification expenses, reputational harm mitigation expenses, victim reimbursement or credit protection expenses. There may also be a deductible.
- if there is no preferred/required vendor list from the insurance company, companies should contact a recommended cyber forensics service

provider to help with a forensic investigation of the scope and severity of intrusion, origin of attack, and remediation.
- consult lawyers to advise on risk mitigation and legal reporting obligations.
- conduct a thorough and in-depth investigation in conjunction with a cyber service provider and legal team.
- document the steps taken.
- preserve (and do not delete) emails or documents that might be relevant to an investigation or remediation, or that might be relevant to the breach in any way. If there is litigation, relevant documents should not have been destroyed.

## CONCLUSION

Cybersecurity should be a primary concern for all companies today. Ransomware and other attacks continued to grow in frequency and sophistication in 2021, with severe economic and financial effects. Cybersecurity readiness entails having organization and technical programs and systems in place, while also being aware of applicable laws and regulations.

Companies doing business in the U.S. must assess applicable cybersecurity laws and legal considerations, including OFAC policies and prohibitions, SEC disclosure requirements, and applicable state cybersecurity and data protection laws. In addition, companies should implement organizational cybersecurity programs and incident response plans which include processes for breach management and reporting, detail cybersecurity compliance measures (including organizational and technical safeguards), and incorporate best practices. If you have any questions or need assistance in connection with these U.S. law issues, or cybersecurity or ransomware generally, it is recommended that you speak with a cybersecurity law attorney. ■

## ABOUT THE AUTHORS

**Matthew Dunn** is a partner in the Cybersecurity and Data Privacy Group, as well as the Litigation Department. Matt is active in the cybersecurity and data privacy arena, counseling clients on best practices and the security risks and consequences they face under the always-evolving regulatory frameworks, such as the EU's General Data Protection Regulation (GDPR) and the various state cyber and data private laws in the U.S. He frequently writes articles on timely cybersecurity and data privacy issues. Matt also maintains an active litigation and counseling practice, primarily focused on complex litigation matters, breach of contract and commercial tort litigation, and trusts and estates litigation, among other areas.
**Email:** mdunn@clm.com

**Guy Ben-Ami** is a partner in the Cybersecurity and Data Privacy Group, as well as the Corporate Department. Guy represents overseas and domestic companies doing business in the United States, helping Israeli and other offshore clients navigate the many securities issues, as well as a variety of other corporate matters and transactions. Guy has represented funds, REITs, startups, venture capital firms and both issuers and investment banks in IPOs and SPAC transactions. A leader of the firm's Israeli Cross-Border practice, Guy is admitted to practice in both New York and Israel.
**Email:** benami@clm.com

## NOTES

1 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

2 https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

3 https://sanctionssearch.ofac.treas.gov/

With a long history of providing legal services to Israeli-based companies coupled with the expertise to steer clients through the legal landscape of the cybersecurity industry, we work with clients who are keenly focused on the future and offer sophisticated advice within a culture that provides innovative problem solving.

**At Carter Ledyard,**
**WE ARE YOUR PEOPLE**


CARTER LEDYARD

WWW.CLM.COM / 2 WALL STREET NY, NY 10005 / T: 212.732.3200

ANTITRUST / ART LAW / CANNABIS / CAPITAL MARKETS / CORPORATE / CYBERSECURITY / EMPLOYMENT LAW
ENVIRONMENTAL AND LAND USE / FINANCIAL SERVICES / INSOLVENCY AND CREDITORS' RIGHTS / INTELLECTUAL PROPERTY / WHITE-COLLAR AND INTERNAL INVESTIGATIONS / INTERNATIONAL BUSINESS / LITIGATION / M&A
REAL ESTATE / SECURITIES / TAX / TAX-EXEMPT ORGANIZATIONS / TRUSTS & ESTATES