GODFREY & KAHN S.C.

Data Privacy & Cybersecurity Flash

May 16, 2017

Christie B. Carrino
414.287.9341
ccarrino@gklaw.com

Cybersecurity alert: Global ransomware threat

Last week, the NHS hospital network in the UK reported a major cyber attack that quickly expanded across the globe, affecting nearly 150,000 companies in 150 different countries. The attack, known as WannaCrypt or WannaCry, originated from a particular form of ransomware targeting "unpatched" and outdated Microsoft Windows file-sharing software. The WannaCrypt ransomware infects devices and then restricts users' access to their files until a ransom is paid. The attack was eventually disarmed; however, experts warn that attackers could slightly modify the ransomware and launch another attack at any time.

Steps to protect your data

While individuals and organizations cannot anticipate and combat every ransomware or other cyber-security threat, there are steps to take that decrease the likelihood of becoming the victim of an attack.

- **Update your software**: Ransomware is most effective at targeting outdated and unpatched versions of Windows Software. Ensuring that your Windows operating system is up to date with the most recent security and software updates, which patch any holes and vulnerabilities in the software, makes it much more difficult for a hacker to infiltrate your system and networks. Keep Windows Update turned on, so that you are automatically prompted to download and install these updates.
- **Avoid clicking on suspicious emails**: Many ransomware attacks are initiated through an infected link in or attached to an email. When a user clicks on the link or attachment, the ransomware is activated on the user's device and then flows through the user's network. Be wary not only of emails from unknown or unfamiliar email addresses, but also unusual or out-of-character emails from those addresses that are familiar. If you are unsure whether an email from a client, colleague, or friend was truly sent by that individual, follow up with a phone call before clicking on any link or attachment.
- **Ensure your information is backed up**: If you or your organization is affected by ransomware, the machine you are using and the files located on its hard drive and/or network may be lost. However, if these files are backed up on an offsite or external storage device, you can access uncorrupted versions of these files on a different machine. Ensuring that your devices and networks are frequently backed up limits the likelihood of a permanent loss of your files and data.
- If your device or network is infected by WannaCry or other ransomware, do not automatically pay the ransom. The hackers do not always release the ransomed

data and files after receiving payment. Additionally, sometimes data can be recovered without paying the ransom. The best course of action is to contact an IT or Cyber Security professional to assist you in analyzing and minimizing the attack.

Godfrey & Kahn's response

Protecting our client's personal and financial data is one of Godfrey & Kahn's top priorities. We employ a variety of measures to help minimize the risk of our systems becoming compromised, including:

- updating and installing the latest versions of Microsoft software;
- ensuring our firewall configuration is up to date and working with our vendor to stay apprised of new threats;
- maintaining an offsite backup of our system data;
- employing email security software, which detects and blocks many types of ransomware and other malware attachments; and
- running reputable antivirus/antimalware software on our servers and devices.

Additionally, Godfrey & Kahn employs a cross-disciplinary team of attorneys who specialize in assisting clients with preventing and mitigating data privacy and cybersecurity threats. To learn more about the various ways our Data Privacy & Cybersecurity Practice Group works to assist clients with cybersecurity concerns, please click here.

Data Privacy & Cybersecurity Practice Group

TEAM LEADERS:

Sean O'D. Bosack
sbosack@gklaw.com

Kendall W. Harrison
kharrison@gklaw.com

TEAM MEMBERS:

Bryan J. Cahill
bcahill@gklaw.com

Christopher M. Cahlamer
ccahlamer@gklaw.com

Christie B. Carrino
ccarrino@gklaw.com

Donald A. Daugherty
ddaugherty@gklaw.com

James A. Friedman
jfriedman@gklaw.com

Kerry L. Gabrielson
kgabrielson@gklaw.com

David J. Gilles
dgilles@gklaw.com

Kristen A. Irgens
kirgens@gklaw.com

Nicholas A. Kees
nkees@gklaw.com

Andrew C. Landsman
alandsman@gklaw.com

M. Scott LeBlanc
sleblanc@gklaw.com

Richard S. Marcus
rmarcus@gklaw.com

John R. McDonald
jmcdonald@gklaw.com

Patrick S. Murphy
pmurphy@gklaw.com

Todd G. Smith
tsmith@gklaw.com

Peter Wilder
pwilder@gklaw.com

Eric J. Wilson
ewilson@gklaw.com