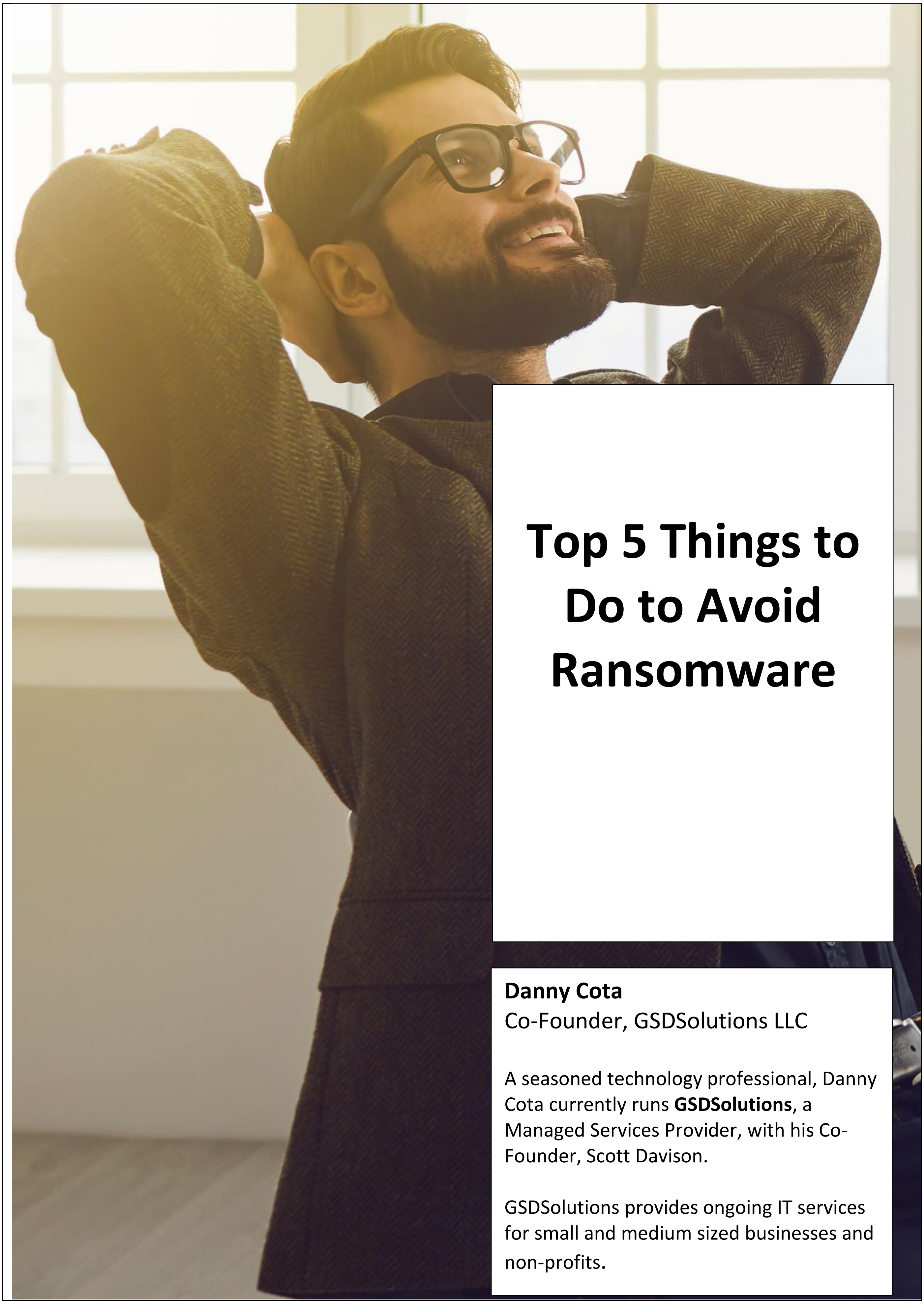
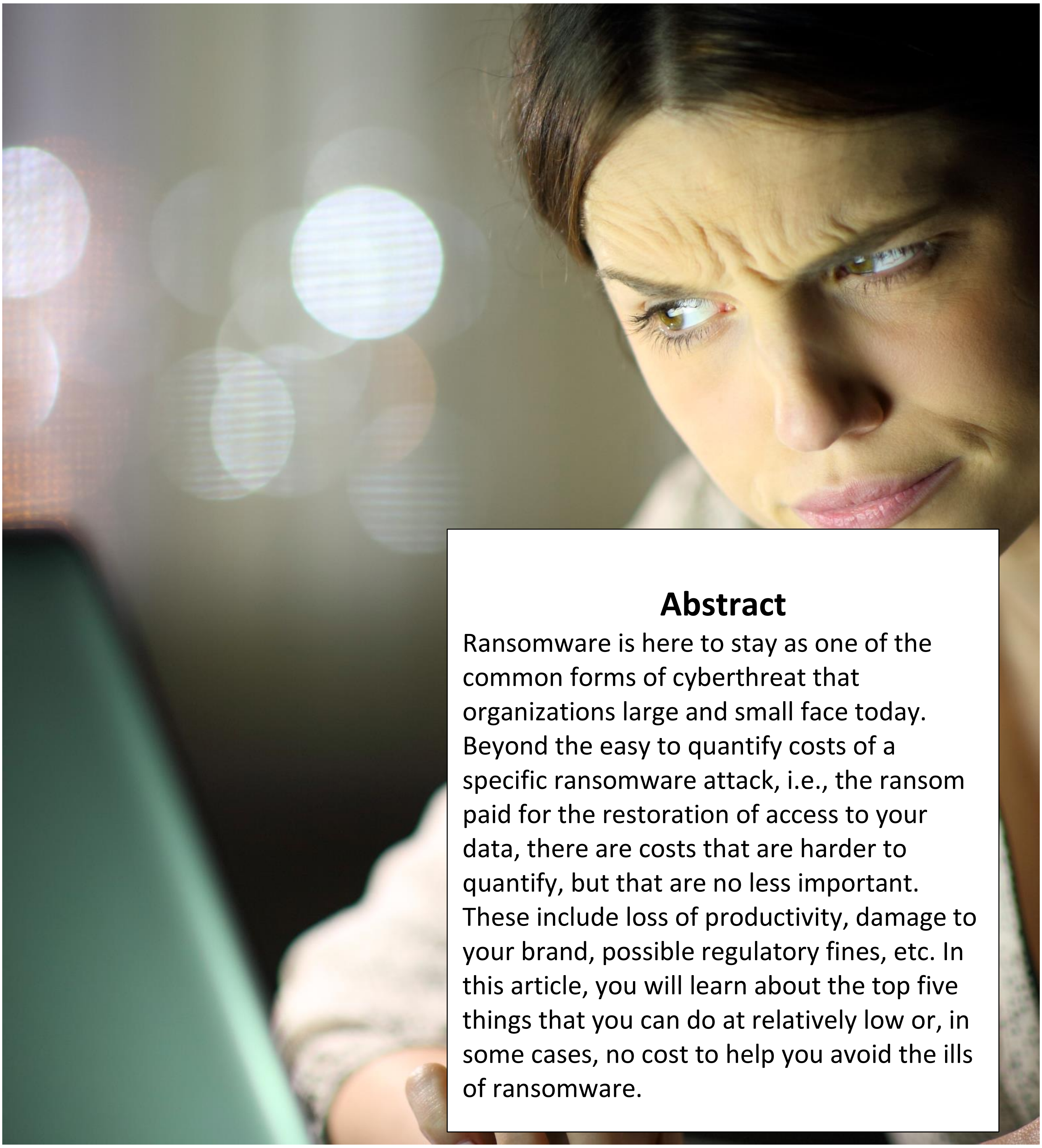


Top 5 Things to Do to Avoid Ransomware

Danny Cota
Co-Founder, GSDSolutions LLC

A seasoned technology professional, Danny Cota currently runs **GSDSolutions**, a Managed Services Provider, with his Co-Founder, Scott Davison.

GSDSolutions provides ongoing IT services for small and medium sized businesses and non-profits.



Abstract

Ransomware is here to stay as one of the common forms of cyberthreat that organizations large and small face today. Beyond the easy to quantify costs of a specific ransomware attack, i.e., the ransom paid for the restoration of access to your data, there are costs that are harder to quantify, but that are no less important. These include loss of productivity, damage to your brand, possible regulatory fines, etc. In this article, you will learn about the top five things that you can do at relatively low or, in some cases, no cost to help you avoid the ills of ransomware.

Introduction

Ransomware is malicious software that is unintentionally introduced onto a computer in order to encrypt the files and folders on that computer. This effectively, locks out the end user from that data. Typically, once a ransomware victim's files have been encrypted, they will receive an email from the ransomware initiator – a.k.a. "hacker" – demanding some form of payment. 99.999% of the time the hacker will request that payment be via Bitcoin or some other cryptocurrency) in exchange for the key (or method) that will allow the user to decrypt their data.

There are a number of variables that can determine the amount that a hacker will demand. For an individual computer owner, that demand may be somewhere in the neighborhood of $5,000. If this same hacker manages to encrypt a large number of individual computers and/or server data in a big organization, then the payment demand can skyrocket to an average of $200,000 to $250,000 (at the time of this writing, May 2021)!

While it may be impossible to completely eliminate the risk of being the victim of ransomware (especially true for a big company), there are at least FIVE things that you can do as an individual computer user to mitigate this risk.

Read on for that list…

Ransomware attacks are costly, but can be avoided!

Antivirus Software

(Often also referred to as "antimalware software" or "endpoint protection.")

- Technical difficulty to implement: **LOW**
- Typical cost: **$3 to $5/month.** (Usually includes protection for 1 - 5 computers.)
- Typical "bells and whistles" for an additional fee:
  - Data backup solution (usually cloud-based)
  - Password management software
  - "Dark Web" monitoring
  - Secure VPN solution
  - Cybersecurity insurance (covering up to some dollar amount in losses incurred by a data breach)

For just a few dollars a month, antivirus software delivers the most "bang for your buck" in terms of managing various data security threats – including ransomware – so it should be your minimal "first line of defense."

Antivirus software is inexpensive and a MUST HAVE for all of your organization's computers!

Do NOT Click on Suspicious Links or Attachments in Email!

- Technical difficulty to implement: **LOW**
- Typical cost: **FREE**
- Typical “bells and whistles” for an additional fee: **Not Applicable**

This may sound like a humorous suggestion, but it isn’t. Most ransomware is delivered (at least on an individual computer-basis) via email, either directly in an attachment, or indirectly in a link within an email. Once the link is clicked on by the intended victim – it then downloads and installs itself.

It’s true that if you have antivirus software installed on your computer, it *should* block the installation of ransomware (or other forms of malware). Nonetheless, you should not rely exclusively on that software to protect you from the unwise habit of opening any and all attachments and/or clicking on links that you receive in email.

Note: Up-to-date Operating Systems – MacOS and Windows – will also try to help you avoid installing malware on your computer by popping up an “are you sure you want to install this software on your computer” message but, again, you should not rely on this exclusively to protect you from these threats.

Be alert when clicking on links/attachments in email… know the source!

DNS Filtering Solutions

- Technical difficulty to implement: **MEDIUM**
- Typical cost: **$1 to $3/user/month**
- Typical "bells and whistles" for an additional fee:
  - Multi-user policy administration
  - Mobile device protection

This software does NOT obviate the need for antivirus software. Rather, it complements antivirus software by acting as a security "backstop" so that if you do inadvertently click on a malicious link (either via email or embedded in a suspicious/compromised web site), this software will intercede by NOT allowing you to actually go to that place on the Internet. These DNS filtering products do this by maintaining a real-time database of known and suspected malicious IP addresses/host names on the Internet.

Note: The technical difficulty of this solution is rated as "Medium" because it often requires "fine tuning" to balance maximizing your protection, while still allowing you to browse legitimate web sites.

DNS filtering solutions are a low-cost – but high value – complement to antivirus software.

Keep Your OS Patched

- Technical difficulty to implement: **LOW**
- Typical cost: **FREE**
- Typical “bells and whistles” for an additional fee: **Not Applicable**

These days, modern Operating Systems (OS) such as Windows, MacOS and Linux all have methods for updating themselves with the latest security patches and OS fixes. Unless you are a VERY advanced user with good reason to disable this automatic updating of your OS, you should leave this feature ENABLED and let your computer perform these periodic updates. OS manufacturers focus on security patches so they can stop new security threats and exploits as they arise.

Note: Most of us have either experienced or know someone who has experienced negative “side effects” from running an OS update on their computer – it happens. That said, the vast majority of OS updates are benign and *should* be applied. Leave your automatic OS updates turned ON and, for good measure, set a weekly calendar reminder for yourself to confirm that your updates are being applied.

Leave your automatic OS updates turned ON!

Backup Your Data Regularly

- Technical difficulty to implement: **LOW**
- Typical cost: **$3 to $10/computer/month**
- Typical "bells and whistles" for an additional fee:
  - Local backup (in addition to cloud-based) storage
  - Multiple-computer backup

Technically speaking, data backup is NOT a method for avoiding ransomware. Rather, data backup offers you the means to recover from a "successful" ransomware attack. If you have a computer and you have data on it that you care about, then backing up that data is simply a MUST DO!

Note: It is important to understand the difference between **backup** and **file-syncing** tools. File syncing tools, e.g., Dropbox, Google Drive, Box, etc., are NOT backup tools! Rather, they are file *replication* tools. This is particularly worth noting as ransomware-encrypted files can be replicated via your file sync tool should you fall victim to ransomware. File *backup*, on the other hand, maintains a discrete history of your backup files, allowing you to restore unencrypted files from previous points in time.

Backup your data. Period.

Final Thoughts

It is worth reiterating that it would be very difficult (if not impossible) to eliminate the threat of falling victim to ransomware completely. That said, the security solutions outlined above are very low cost (or FREE) and should be implemented on every computer that has valuable data on it to avoid falling victim to ransomware.

Also, the solutions that we've discussed here are largely focused on protecting an individual computer from the threat of ransomware and other malware, but there are more advanced enterprise security solutions that go even farther than our five recommended solutions, but these go beyond the scope of this document.

Avoiding ransomware can be done regardless of your budget.

Still Have Questions? We're Here to Help!

Should you have any questions about the technologies discussed here (or any other technology-related questions), please email us at **getstuffdone@gsdsolutions.io** or call us at **(650) 282-7695**.

About GSDSolutions

Simply put, GSDSolutions is a customer service company. True, our particular flavor of customer service happens to center around technology – computers, software, cybersecurity, etc. – but, ultimately, our job is to serve our customers. We serve our customers in the same way that we would want to receive services ourselves – that is, with integrity, with wisdom and a dash of empathy thrown in for good measure.

gsdsolutions

https://gsdsolutions.io/