IDC PeerScape

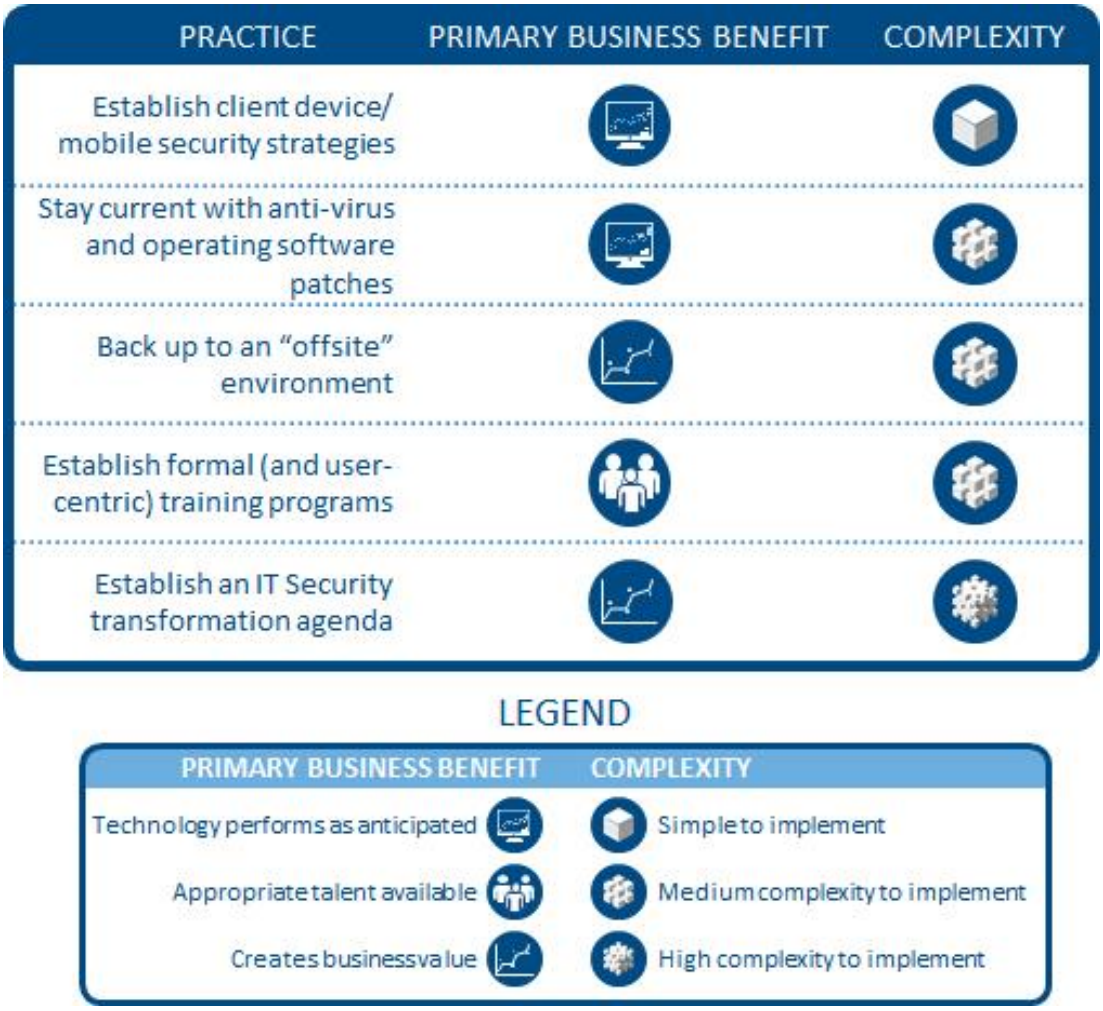
IT Security: Ransomware

Simon Piff

IDC PEERSCAPE FIGURE

FIGURE 1

Best Practices to Avoid Ransomware



PRACTICE	PRIMARY BUSINESS BENEFIT	COMPLEXITY
Establish client device/ mobile security strategies	🖥	■
Stay current with anti-virus and operating software patches	🖥	▦
Back up to an "offsite" environment	📈	▦
Establish formal (and user-centric) training programs	👥	▦
Establish an IT Security transformation agenda	📈	✱

LEGEND

PRIMARY BUSINESS BENEFIT		COMPLEXITY	
Technology performs as anticipated	🖥	■	Simple to implement
Appropriate talent available	👥	▦	Medium complexity to implement
Creates business value	📈	✱	High complexity to implement

Source: IDC 2015

IDC OPINION

IT industry security experts have acknowledged ransomware is on the rise. Due to the ease with which cybercriminals subscribe to services that deliver ransomware to a broad range of targets and in the process earn significant sums of illegal income, Interpol — the global intergovernmental organization that facilitates police cooperation — has identified this cybercrime as one that needs particular focus.

Ransomware is particularly insidious since the process — one that encrypts files on your device until payment is made to the attacker, who may or may not provide the key to unlock your data — could potentially stop some businesses from being able to operate and so demands specific attention.

IN THIS STUDY

In this IDC study we present five practices that all organizations should implement in order to avoid being infected by the most insidious malware currently circulating online: ransomware. The study will help CIOs understand the importance of device security in the greater field of overall IT security, and will also help IT security professionals better grasp the impact of staying current with software patches as well as help end users understand why IT security training needs to be perceived as a business-enabler and not merely as another cumbersome process that slows down productivity.

Even as the implementation of firewalls, anti-virus software, and software patching is not a new phenomenon within organizations, growing incidence specifically around ransomware demands that organizations educate themselves on the impact of this type of attack and the fact that, unlike other types of virus circulating online, ransomware could prove to be lethal to some business organizations should they fall foul of this type of attack.

Although the process of the attack is a virus that, through complex encryption, denies the device owner or administrator the ability to access the data on the device, there is a further concern in that not all attackers are being "honest" enough to provide the keys to unlock the data rendering the device — and in many cases the backed-up data — useless to the owner. Should this happen to a smaller organization with no offline backup facilities, it could potentially end the existence of such an organization.

Another form of ransom is through ongoing denial of service (DoS) attacks, and though this is acknowledged as a form of ransom, it is not the subject of this study.

SITUATION OVERVIEW

Ransomware is not new, having first been identified in 2009, but a growth of 165% in attacks was seen in the first quarter of 2015. It's only a matter of time before more organizations start to report on this issue, and so having a solid defense strategy in advance of this anticipated onslaught may help many organizations avoid this particular type of attack.

Online activity is only set to grow globally with more businesses conducting more business online using a wide range of devices; the levels of interconnectivity this demands will ensure that the potential to be infected will grow. The initial financial impact of such infections has, to date, been limited, with many threat actors asking for only a few hundred dollars from individuals and a few thousand from organizations. Interpol, however, has identified this type of attack as particularly insidious since it a) creates a valuable, substantial, and repeatable revenue stream to criminal organizations (one IT security firm estimates a successful attacker can earn up to US$394,000 in a single calendar month!), b) it has the potential to cripple a smaller organization, and c) it is a type of attack that has an entire ecosystem behind it: the engineer that writes the malware, the organization that markets and provides the service, the organizations that delivers the malware and the process by which payment is made (usually through using Bitcoin). As such it has the potential to become a significant menace in the future if it is not dealt with early and effectively, and there is absolutely no guarantee that once an organization or individual has paid the "fine" to decrypt their data they will not be attacked again by the same or a different group or organization.

From an IT management perspective there is a view that ransomware is the same as any other malware being circulated online today, and though the delivery mechanisms are very similar (e.g., either through infected websites or as an email attachment) due to the nature of the attack the financial impact can be far more significant than a single user having their hard drive locked out. Some of the more advanced malware programs have the ability to encrypt not only the data on an end-user device, but also the backed-up data on the network. There are already some packages that can search out and encrypt data on networked devices and shared resources on the local area network. It will only be a short time before the package will be redesigned to seek out other data on the network, which could have disastrous results for the infected organization.

A far more stringent approach needs to be taken due to this new breed of malware and the new and improved methods of distribution available to the attackers, and this needs to include not only the necessary technologies and tools to diminish the ferocity of such attacks, but also the urgency of the need to educate end users on what to look out for.

Practices

Practice 1: Establish Client Device/Mobile Security Strategies

Problem

Ransomware enters the organization through the end-user devices. The proliferation of mobile devices — be they tablets, laptops, or smartphones and similar form factors — in all organizations can make securing them a far more challenging process than in the past, where devices were permanently connected to a physical network.

Anti-virus is widely deployed in most enterprise mobile devices, but as bring your own device (BYOD) becomes more prevalent than choose your own device (CYOD) or employer-provided systems combined with the explosive adoption and use of smartphones in the business environment, securing these devices becomes a more challenging proposition. Embracing the various productivity tools used by the workforce, and then providing tools and systems that can help secure these various resources from malware attacks is a more realistic approach than trying to restrict usage of tools to a few, but will require advanced mobile device management strategies that go beyond simple anti-virus.

Since some ransomware variants will go as far as to lock down access to backed-up data, with others even going as far as to try to delete backed-up data, the ability to rapidly detect ransomware on a device and to quarantine it so as to limit the damaging effect of the malware is going to become a critical business requirement. This may well demand the need for an application or agent to sit on the device in question and be in touch with a trusted command and control module either hosted within the organization's datacenter, or be subscribed to as a service that can help identify such malware, since many of the current mobile device management solutions may not be sophisticated enough to be useful in stopping the impact of ransomware. It may be further required that all mobile devices are quarantined in some form or other to ensure that the malware is contained and is unable to spread to other devices on the network.

This leads to a need to consider device management by user profile. For example, quarantining the device of an employee who needs fast and seamless access to the network will not be an acceptable business practice, so such device management strategies need to consider both the needs of the individual in their role in the organization and weigh the risk to the organization should such a machine become infected, and how that could impact the larger business organization should that infection spreads.

The solution for mobile computing management has been available for many years now, but smartphones and tablets, especially in a BYOD environment, are something less understood. Dowling Aaron is a private law firm in the United States that experienced a sudden increase in demand for mobile device connectivity to the corporate network that surpassed the ability of the company's IT team to manually service. Because of the potential for device loss and theft, a solution to manage the growing number of devices was sought. The eventual solution that was implemented was able to deliver the following benefits:

- **Basic mobile device security:** The ability to set a security and passcode policy (passcode requirement and maximum number of attempts) outside of user control
- **Protecting personal data:** Ability to remove only corporate data, leaving any personal data intact
- **Securing multiple device types and operating systems:** Evolving support for any mobile device type, along with different versions of Android and Windows
- **Flexibility to add new capabilities:** A feature specifically for disaster recovery purposes. Although the firm has data backup to one of its facilities the firm uses the solution to distribute an updatable list of employee contacts and procedures to users' mobile devices

The balance between the demands of the organization and the needs of the individual, especially when considering members of the C-suite and key knowledge workers, may need to be evaluated individually and not be assigned to an automated process.

Practice 2: Stay Current with Anti-Virus and Operating Software Patches

Problem

Cybercriminals operate in much the same manner as businesses, in that they are constantly changing their systems and processes to stay ahead of the "competition" and in this case the competition is about detection. Malware is frequently modified and updated simply to avoid detection by anti-virus software. Similarly, software (from applications to operating systems) are constantly issuing new patches to fix security and other issues that emerge and with as many as 24 zero-day vulnerabilities reported in 2014, in many cases there is no fix for the security vulnerability exposed.

Although some of the ransomware attacks leverage known malware, which can be thwarted by standard signature-based anti-virus solutions, many are using new and unknown variants that can bypass these simple controls, so a much more layered approach is required.

Ransomware is delivered through both web and email, and as such ensuring these two critical applications are sufficiently protected from a security perspective is paramount. Whitelisting, containerization of applications, and network segmentation are some of the processes that will need consideration in order to protect the organization, but at the same time a clear process of ensuring anti-virus and software patches are kept as current as possible, with minimal user-intervention or overhead, are equally important.

Castilla-La Mancha from Toledo, Spain is responsible for the communications infrastructure, systems, data processes, and user support for the entire regional government — some 10,000

PCs located in five separate locations. By deploying a centrally managed endpoint protection solution the organization is able to ensure these PCs and their server infrastructure are protected with the latest anti-virus and malware avoidance solution that supports both physical and virtual PC and server environments across multiple operating systems. This centralized approach has also helped the organization reduce the physical footprint and resource requirement within the IT security department, while ensuring the highest levels of security are maintained. The implementation of centralized endpoint security solutions has resulted in reduced downtime, enhanced efficiency, and a reduction in staff hours that were previously devoted to dealing with spam and viruses.

Automating update processes becomes more challenging as more bespoke applications appear within the environment, so ensuring an enterprise architecture that can limit the need for custom-coding as much as possible means that the IT security professionals need to interact at length and in depth with the broader IT and business teams to the point that the business is able to identify a risk-based decision-making process around the architecture that can address the needs of the business in view of what is technically possible, and provide a judgement-based response to any custom-coding requests.

A U.S.-based pest control company implemented an automated server patch management solution that would extend beyond just straightforward Windows patch management to embrace a range of other often-used technologies in the server environment. The one selected also offers a "planning mode" permitting the organization to simulate patch roll-outs in order to identify and eliminate any issues ahead of time, a critical component in many environments.

Practice 3: Back Up to an "Offsite" Environment

Problem

Certain types of ransomware are able to encrypt your backup files, or to live within your backup environment only to reappear when the files are restored from backup.

Backing up to an offsite environment permits the opportunity to have a disaster recovery site for your disaster recovery. In simple terms the process permits you a tertiary layer of security should you find that your backup is infected, and would allow organizations the ability to seek out and clean the offsite backup from the malware.

One such organization is a law firm specializing in aircraft sales. For them, communications is the key to serving their clients, and email is the basis for much of their customer interaction. A company spokesman was quoted as saying, "Without [email], we can't close deals and get planes delivered on time." Moving from a tape backup environment to an offline one the organization has enjoyed a much more secure backup environment for email and databases as well as greater efficiencies through automation of backups, and drastically reduced recovery times.

For a number of organizations around the globe there is a belief that offsite backup is not permitted due to a range of legislations, especially within the financial services and other highly regulated industries. For the most part this is a misinterpretation of guidance being given and even as there are strict laws governing privacy of personal data and integrity of financial information, the ability to leverage an offsite environment for the purpose of maintaining a backed-up copy of this data should — assuming all the necessary safeguards are in place — not be impossible.

In an ideal world, the types of data that should typically be found on a mobile device should not be the types of data that fall under these levels of jurisdiction, instead being confined to the databases and applications that create, host, and analyze this information, and so the issue of offsite backup for mobile devices complying with legislation should not be a material issue. In reality this data frequently finds its way onto mobile devices anyway, which, in many cases, could be in contravention of the regulations, which is a more serious issue in the first instance, and one that is not covered within this document.

Practice 4: Establish Formal (and User-Centric) Training Programs

Problem

IT security is generally seen as an obstruction to achieving higher levels of productivity. Although more senior members of an organization may understand the need for higher security levels, quite often this is also the group of people most in need of personalized security policies. For the "generalist" employee, stringent security controls can been seen as an inhibitor to workplace effectiveness and this can often result in the process being circumvented to make things "easier" (a classic example being the laptop password written on a sticky note pasted to the machine).

IT security policies need to become more effective, but at the same time should not negatively impact productivity. This requires the need to create a "culture" of IT security (which may well need to extend beyond just IT).

In the realm of ransomware, explicit training would make more sense, to educate users on the need to become more vigilant over websites and email attachments. Very few organizations offer training on what a good or bad email looks like, and yet the process can be vastly simplified with a few pointers on what to look for by looking at the sender and validating (through both a degree of common sense and some IT pointers) the sender's address with regards to the message being sent. Checking the file extension of any attachments is also important as many malware files "pretend" to be an image or a document. Many phishing emails are embedded with hyperlinks that will take you to another site (and some may then ask for a username and password), but here many email clients will let you view the hyperlink address prior to clicking – allowing the user to evaluate for themselves whether this is a legitimate message with a legitimate link.

Many forms of ransomware do not use any sophisticated device, simply relying on user ignorance to download innocent-looking files that have a malicious workload that launches when the files are clicked on. In some cases simply landing on a compromised website can trigger an infection, so knowing what types of sites and files are safe and what are not can be a major challenge.

Two global organizations address this problem with different approaches. The first, a global software company, uses web-based training on a semi-annual basis to "certify" that all staff are appraised of the latest security requirements. The process involves taking an online test that reaffirms the main aspects of personal responsibility for password protection, device physical security as well as the various forms of web and email threats. In order to maintain access to critical systems all employees need to pass this online "examination."

Another example is a global logistics organization that takes a less onerous but more direct approach, by hosting internal security days for its employees in the form of an internal "event" with speakers and presenters from external organizations adding value to the internal IT messaging around their specific security needs.

The process for improving the security quality of email use and web surfing is not complicated, but is rarely explained to the users in a manner that is easily comprehensible and that is a non-obtrusive way to improving both security and workplace productivity.

Practice 5. Establish an IT Security Transformation Agenda as Part of the Broader Governance Framework

Problem

IT security is not an end-state. Unlike almost any other IT project, there is no endpoint (nor any end in sight) with regards to what is required to maintain security at the highest levels for as long as is possible. The need to constantly evaluate, mitigate, and remediate is critical to all organizations, and in the field of ransomware this also means constantly educating the workforce on new malware and processes as they emerge.

IDC has developed its own *IT Security MaturityScape* (**http://www.idc.com/getdoc.jsp?containerId=247584**), a document that helps organizations both benchmark themselves with regards to where they lie on an IT security maturity curve, but one that also provides critical advice at each stage of the maturity around people, process, and technology that can help organizations understand more clearly what it means to be optimized for IT security in today's world.

A government CIO office in the Asia/Pacific region has established a comprehensive governance mechanism based upon globally recognized standards and runs compliance training and audits on a regular basis. At the same time it has developed a comprehensive self-assessment framework for its bureaux/departments for its maturity levels in information security management for continual improvement. While in the United States, a large aircraft manufacturer has stated,

> We have supported and contributed to the NIST Cybersecurity Framework (CSF) (**http://www.nist.gov/cyberframework/**) from its inception. We use it as a basis to assess the overall security of both internal organizations and with external customers. The CSF promotes a comprehensive, adaptable, risk-based approach that is technology- and regulatory-neutral. As we have used the Framework, the results have had significant impact in explaining issues and setting the direction for future cybersecurity capability.

A well-known global IT security vendor built a local "virtual" response team soon after Cryptolocker attacks started targeting Australia. The virtual team allows timely notification and response across different internal business units including Incident Response, Managed Security Services, Product teams, Sales Engineers, Security Technology and Response (STAR) to aid in proactive notifications to customers, recommended steps to reduce risk, campaign research and identifiers, update of signatures, behaviors for blocking, and detection mechanisms. The organization recommends that similar virtual teams be established within a customer environment to facilitate fast response across relevant business units – Security, Infrastructure (endpoint, backup), Networks, Public Relations, and Executives, for example. In addition, the organization speaks with its respective security technology vendors to understand how it can help as a part of this process.

Although ransomware is, for now, mostly limited to endpoint devices and the impact of being locked out of access to files on laptops and personal computers, a more holistic IT strategy that encompasses the broader organization is required to ensure that as this type of malware evolves and looks for more rich targets behind the firewall, organizations are not blind-sided and do not suffer business-critical failures due to inaccessibility of data housed within critical systems. This will require a far more reaching security architecture that demands a more meaningful understanding of the critical applications and systems, where the data for such applications reside and the interreliability of systems in order to ensure business continuity is not affected.

FUTURE OUTLOOK

Currently ransomware is mostly targeting personal computing devices such as laptops, desktop computers, and tablets since, for now, these are where several of an individual's critical files are located. Files such as financial records, correspondence, and photographs are important to an individual, but over time these types of files will be either located on, or accessed by, a mobile device such as a smartphone or a tablet. It's clear that these devices will become attack vectors in the not-too-distant future and that in this scenario, the ease with which applications are downloaded from stores and installed — and the fact that many such applications are hosts to malware already — indicate that it would be all too easy to lock a user out of their smartphone.

Ironically in its favor is that this is likely the only device a victim can use to respond to the criminals' demands for money to unlock an encrypted hard drive, although ransomware for some phone operating systems are already in existence — but ultimately, unless law enforcement can do more to track members of the ecosystem and have them pay for their crimes, the income potential versus the investment is likely to be just too strong a motivation, so smartphone and phablets will likely become the next "low-hanging fruit" for the attackers.

More insidious and concerning is the idea that an attacker merely uses the end-user device as a vehicle to get inside a larger organization and attack, say, a general ledger or customer information database. The potential impact on an organization of any size would be considerable and the corresponding cost to have such files unlocked would no doubt be commensurate. Ensuring this scenario never happens must be the primary concern of all security architects, and ensuring any such attacks are limited to personal devices alone must still remain a key attribute of defeating such an attack.

Resolving the issue of such attacks will continue to be the task of relevant legislative authorities, but the dispersed nature of the Internet combined with various gaps in legislation make the job of the law enforcement agencies extremely challenging. Governments will need to take on a more global view in combatting cybercrime if they are to be more successful, but gaining agreement between nation states on this will be enormously challenging, allowing the criminal ecosystem — since it is more of an industry than merely a handful of players — to find loopholes and continue to operate. The chances of ransomware disappearing anytime soon is improbable, meaning that organizations of all sizes will need to implement a range of technologies and processes to ensure they can limit the impact of such attacks.

SUMMARY OF PRACTICES

The best practices described in this report summarize five key initiatives that organizations can undertake to minimize the impact of a particular type of malware, that of ransomware:

- **Establish client device/mobile security strategies.** Mobile devices such as laptops, tablets and increasingly, smartphones, are now critical productivity tools in many organizations, and so ensuring they are sufficiently protected physically, and are "known identities" to corporate networks will become more critical to ensure business continuity. Different members of the organization will need differing levels of security and quarantine. Understanding this will help assure the business that IT security is as much about productivity as it is about securing the environment.
- **Stay current with anti-virus and operating software patches.** Staying up to date in this mobile world can become more challenging as corporate policy is not always enforced unless physically attached to a corporate network. Such processes need to evolve to be able to ensure the mobile device can be maintained "as current as possible" even in its remote state.

- **Back up to an "offsite" environment.** Ensuring back up regimes are adhered to will become the critical differentiator between those that can successfully recover from ransomware and those that cannot. Since some versions of this malware can also infect backups, having a tertiary level of offsite backup can provide a further degree of insurance that clean and non-infected files can ultimately be recovered.
- **Establish formal (and user-centric) training programs.** Very few employees are ever trained to understand how to avoid bad emails or attachments nor how to avoid unsavory and unwanted hyperlinks. Such training will need to become an ongoing part of any mature IT security framework.
- **Establish an IT security transformation agenda as part of the broader governance framework.** IT security is not an end state, but a constant process that needs the right level of technology and process and the right levels of engagement with people. To assist in a better understanding of this IDC has created its own *IT Security MaturityScape,* which shows how organizations must commit to IT security, with specific guidance at each of the five different stages of maturity.

LEARN MORE

- *IT Security MaturityScape* (IDC #247584, March 2014)
- Interpol Cybercrime Unit. http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
- Castilla-La Mancha http://www.symantec.com/content/en/us/enterprise/customer_successes/b-castilla-la-mancha-CS-en-us.pdf
- Cybersecurity Framework http://www.nist.gov/cyberframework/

Synopsis

Ransomware is rapidly emerging as a new variant of malware that can wreak havoc on personal productivity by locking users out of their own files until a "ransom" is paid to the attacker. Even then, not all attackers will release the files, and so a more targeted approach to dealing with, and hopefully avoiding, the impact of ransomware is called for. This report provides five best practices that organizations can adopt to reduce the potential impact of this particularly insidious type of attack.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Asia/Pacific Headquarters (Singapore)

80 Anson Road, #38-00
Singapore 079907
65.6226.0330
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice