@ISACA Volume 7 6 April 2016

In This Issue

5 Key Considerations When Preparing for a Ransomware Incident

SHARE

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

Ransomware attacks are on the rise and likely to become more painful and frequent as attackers are finding that organizations are not well prepared to defend themselves and are often willing to pay handsomely to end the incident. Ransomware attacks commonly include an attacker using malware software or code that both encrypt data files with strong encryption and replicate and propagate themselves quickly throughout networks to maximize their presence and impact. The attacker will harvest the encryption keys needed to decrypt the data and hold onto them in exchange for ransom. If victims do not pay, they will not be provided the encryption keys required to decrypt and access their data.

Organizations that consider the threat of a ransomware attack to be both likely and materially business impacting should consider a number of issues to limit the impact of these attacks and respond effectively. Here are 5 key considerations when evaluating this threat scenario and response plans:

1. **Managing the Risk: To Pay or Not to Pay?**—One of the most difficult decisions that an organization has to make is whether or not to pay the attacker to gain access to encryption keys or the other methods to regain access to its data. Often, organizations pay only as a last resort, but it is a risk-management decision that needs to be considered carefully. In some cases, it may be economically and operationally more efficient to pay the fees to gain access to data than it is to try to restore data and systems. That said, if an organization pays and it becomes known either to the attack community and/or the public, the organization may become the target of similar attacks due to the perception that it paid once and may do so again.

   The decision to pay or not to pay should be considered by decision makers prior to an attack. Organizations should establish thresholds to identify their risk appetite for this type of situation, and factors such as loss of productivity, availability of data, reputational impact and cost of recovery should be considered. These thresholds should be designed to establish both at what point in the attack and at what price it is favorable to pay.
2. **Negotiation**—It is often the case that a ransomware attack will include a demand for large amount of currency, often Bitcoin, to provide the mechanism to release the data. If an organization decides that it is willing to pay the attacker, it should engage in a dialogue with them, if possible, to negotiate the fee. The adversary is often more interested in getting some money rather than no money. The fee that an organization is willing to pay should be based on the projected costs of remediation of the incident without the help of the attacker. If the organization is able to negotiate a fee that is lower than this cost, the decision to pay may be an easier one.
3. **Is this the beginning or end of the attack**—Recent attacks have demonstrated that attackers are using ransomware-style attacks as the last module of a multifaceted attack strategy. The encryption of data can be used to distract an organization from other attack actions and activities and to cover the attacker's tracks as they are trying to escape with data assets or implanting malware tools to be used in the future. Ransomware attacks are obvious and intended to make it known that the adversary has successfully exploited the organization. It is important to recognize that the remediation of a ransomware attack should always be followed up with a thorough investigation to ensure that the attacker did not carry out any other malicious actions as part of their attack or leave capabilities behind to carry out the same attack in the future.
4. **Are backups good enough and should they be used?**—Often, the way organizations recover from a ransomware attack if they choose not to pay is to restore their data from backups. This assumes that the backups are comprehensive, have integrity and are recent enough to be useful to the organization. It is important for an organization to consider whether its backups are already infected with the attack malware/code or if the backups are susceptible to being affected by the original attack. A sophisticated attacker will implant their attack capabilities on systems and allow them to lay dormant for a significant period of time, hoping that they will propagate throughout the backups of the organization. Once the backup is restored, they will attempt to use their attack method again.

   One way to defend against this scenario is to only backup data files and not system files to limit the possibility of reinfection. The attack code may be included in the data files, but an action would have to occur for it to be installed and operate again. Ideally, the method of exploitation and attack would be positively identified prior to recovering the backups.
5. **Identify when networks and systems should be segmented and/or disabled**—Malware/attack code associated with ransomware activities often attempts to replicate and propagate itself across systems and networks as fast as possible to increase its effectiveness. In many cases, organizations use resources such as shared storage and network file shares that are easily leveraged by modern ransomware tools, such as the popular Cryptowall. It is important to identify when it is appropriate to segment and/or disable networks and systems to contain the attacker. Doing so can have significant business impacts. The conditions and scenarios that qualify for these actions should be discussed and agreed upon in advance with business process owners and leaders.

Preparation is key to a successful response for any attack scenario, but especially for a ransomware attack. These attacks and the decisions and actions that an organization is required to take to effectively respond to them go well beyond technical considerations and often fall into the realms of both enterprise and information risk management. Regardless of what decision is made, business leaders need to be aware of the broader considerations associated with this type of attack to ensure they are not targeted by the original or different adversaries in the future.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.

Report of the Nominating Committee

SHARE

By Ken Vander Wal, CISA, Nominating Committee Chair

The charge of the ISACA Nominating Committee, as described in section 5.2 of the ISACA bylaws, is to prepare a slate of candidates for the ISACA Board of Directors, consisting of a board chair, vice-chair and up to 6 directors, for review by the association membership. The Nominating Committee is chaired by a past chair of ISACA, and its members include 2 additional past chairs and 4 other members with significant ISACA experience and diverse geographic representation.

The committee takes very seriously its obligation to prepare the best possible slate of individuals who will work together as a team to lead the association. Its evaluation of candidates takes into account their intent to reflect the organization's diversity in terms of geography, skills, experience and other relevant factors, while also balancing continuity and new viewpoints.

The selection process is managed with attention to detail. Deadlines are strictly adhered to, nominations are treated with unbiased consideration, candidates are interviewed and strict confidentiality is maintained throughout the process. The Governance Committee (GC) provides oversight to the committee's processes and the committee reports to the Board of Directors and the membership of ISACA.

The 2015-16 Nominating Committee is pleased to present the slate for the 2016-17 ISACA Board of Directors. As chair of the committee, I affirm that the committee's deliberations were carried out in accordance with the bylaws and good governance principles.

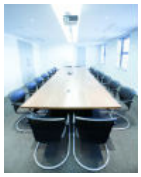
2016-17 Nominating Committee Members:

- Ken Vander Wal, Chair. CISA, CPA, USA (past chair)
- Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Australia (past chair)
- Greg Grocholski, CISA, USA (past chair)
- John Ho Chi, CISA, CISM, CRISC, CBCP, MBCP, Singapore
- Urs Fischer, CISA, CRISC, CIA, CPA, Switzerland
- Gloria Cardenas, CISA, CGEIT, Colombia
- Vernon Poole, CISM, CGEIT, CRISC, CIPFA, United Kingdom

Slate of 2016-17 Board of Directors

SHARE

ISACA News



Source: ©iStock.com/ MickyWiswedel

ISACA will hold its Annual General meeting on 25 June in Chicago, Illinois, USA, where it will install the 2016-17 Board of Directors. In accordance with the association's bylaws, the Nominating Committee submits the following slate as the proposed 2016-17 Board of Directors:

- Christos Dimitriadis, Ph.D., CISA, CISM, CRISC, ISO 20000 LA, chair
- Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, vice-chair
- Rob Clyde, CISM, director
- Leonard Ong, CISA, CISM, CGEIT, CRISC, COBIT 5 Implementer and Assessor (Singapore), CFE, CFP, CGFA, CIPM, CIPT, CISSP ISSMP-ISSAA, CITBCM, CPP, CSSLP, GCIA, GCIH, GSNA, PMP, director
- Andre Pitkowski, CGEIT, CRISC, COBIT 5 Foundation, CRMA, OCTAVE, ISO 27kLA, ISO 31kLA, director
- Edward Schwartz, CISA, CISM, CAP, CISSP, ISSEP, NSA-IAM, PMP, SSCP, director
- Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, director
- Tichaona Zororo, CISA, CISM, CRISC, CGEIT, CIA, CRMA, director
- Robert E Stroud, CGEIT, CRISC, past chair
- Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, past chair
- Greg Grocholski, CISA, past chair
- Matt Loeb, CGEIT, CEO and director

The bylaws grant the chair the authority to augment the board by a limited number of appointments if desired. Christos Dimitriadis has proposed the appointment of the following individuals to serve as directors on the 2016-17 Board of Directors, subject to approval by the board: Zubin Chagpar, CISA, CISM, PMP, R.V. Raghu, CISA, CRISC, and Jeff Spivey, CRISC.

Included on the agenda of the Annual Meeting of the Membership will be the annual report, the treasurer's report and comments from the chair of the Board of Directors.

All ISACA members are invited to attend the Annual Meeting of the Membership.

ISACA Annual General Meeting to Take Place in Chicago

SHARE

ISACA News

The ISACA Annual General Meeting (AGM) takes place to instate the Board of Directors. Those who attend this meeting will also be able to review fiscal information from the past year. Attendees will have the opportunity to receive ISACA's annual report, which will be posted on the ISACA web site after the meeting. The AGM will take place on 25 June at the Langham Hotel, 330 N. Wabash Avenue, Chicago, Illinois, USA. This meeting will take place at 8AM CDT (UTC -5 hours).

To register to attend the meeting, email your name and member number to agm@isaca.org. To learn more about the meeting, visit the ISACA Annual General Meeting page of the ISACA web site.

June Exam Deferrals

SHARE

ISACA News

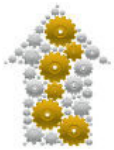
June exam deferrals are currently open. June Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) exam candidates can either defer their exam to September 2016 (exams offered at limited sites) or December 2016. June Certified in the Governance of Enterprise IT (CGEIT) and Certified in Risk and Information Systems Control (CRISC) candidates can defer to December 2016.

Deferral requests received on or before 22 April are charged a US $50 processing fee. Requests received from 23 April through 27 May are charged a US $100 processing fee. Requests received from 28 May through 8 June are charged a US $125 processing fee. After 8 June 2016, no deferrals are permitted.

Transforming the IT Audit Function—Taking the Digital Journey

SHARE

ISACA News



Source: ©iStock.com/lvcandy

Digital disruption is changing the way many aspects of how an organization function, including IT audit. *ISACA Journal* volume 1 author Robert Kress shares lessons learned during Accenture's IT audit transformation:

- **Align IT audit strategy with business strategy**—In today's business environment, corporate strategies can change frequently in response to market pressures, competitive challenges or emerging technologies. IT capabilities and the IT audit function need to be just as nimble in adjusting to the changing needs of the business and new technologies.
- **Clarify governance**—It is critical to have senior business leadership input on new and changing risk factors resulting from changes in business strategy, IT audit's assessment of risk, and high-level internal audit (IA) plans. This demands a more robust governance regimen in which input is solicited from business leads on a near-continuous basis, rather than once a year.
- **Run IT audit like a business**—Operate the IT audit function like a business, and treat the people and organizations served as true customers. Provide these customers with a set of defined service offerings in a "managed service" approach, so they can request the services they want based on the changing needs of the business. Focus relentlessly on value-add to the business, and measure customer satisfaction.
- **Manage performance metrics**—Measure critical success factors, benchmark progress and use the overall metrics to drive change. The role of IT audit leadership is critical here, intervening where necessary to rectify deficiencies and capitalize on achievements.
- **Transform people**—An integral part of transforming the function may involve transforming the people and the internal culture in which they are working. An audit function that historically has been retrospective needs to undergo a radical shift when moving to a proactive stance. Strong leadership is required to drive culture and process change, so be sure to have the right people in senior management positions. Work to instill new ways of thinking and working throughout the function.
- **Go big**—Make bold decisions to drive step-function increases in the enterprise's capabilities, and apply rigor and discipline in executing the changes. Be just as tough on the internal business processes of IT audit as on the business areas tasked with auditing.
- **Communicate success**—This, along with benchmarking, is helpful to demonstrate the value IT audit adds and the progress being made to senior leadership as well as the IA team. Do not be embarrassed to speak highly of the IT audit function when meaningful and measurable progress is achieved.

Read Robert Kress' full article, "Transforming the IT Audit Function—Taking the Digital Journey," in volume 1 of the *ISACA Journal*, in which you will also find additional coverage of timely and relevant issues affecting the ISACA professional communities. Kress will also lead a session titled "Transforming Internal Audit: A Digital Journey" at the North America Computer Audit, Control and Security Conference (CACS).

VIEW ARCHIVES PREVIOUS ISSUE NEXT ISSUE