CYBERSECURITY ESSENTIALS FOR PHILANTHROPY

Handbook for Security Policies, Tools, Practices, and Training

Published on September 24, 2019

Charles Boname
Director, Information Technology, Vancouver Foundation
Dan Callahan
VP of Global Services, CGNET

TECHNOLOGY AFFINITY GROUP

One North State Street, Suite 1500
Chicago, IL 60602

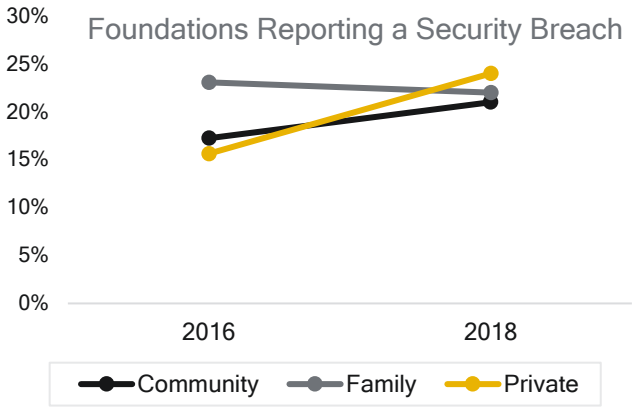
info@tagtech.org

OVERVIEW

PRAGMATIC INSIGHT FROM IT LEADERS IN PHILANTHROPY

Executives in philanthropy are increasingly concerned about cybersecurity. Phishing attacks are weekly, if not daily, and the stakes of a breach are high. In spite of our best attempts as a sector to develop robust practices, 21% of respondents to TAG's 2018 State of Philanthropy Tech survey reported experiencing a security breach in the past two years. For private independent foundations, the breach rate was even higher at 24%. No wonder there's growing concern.

Through the *CyberSecurity Essentials for Philanthropy* series, we aim to reduce your organization's risk and establish best practices throughout the sector.



Source: 2018 State of Philanthropy Tech Survey, available at http://www.tagtech.org/philanthropytech2018.

This publication offers best practices and suggestions based on the collective on-the-ground knowledge and experience of your peers at philanthropic organizations across North America. On behalf of the members and directors of the Technology Affinity Group, we're grateful for the authors' generosity and expertise.

JAMES R. RUTT
Chief Information Officer, Dana Foundation
President, Board of Directors, Technology Affinity Group

CHANTAL E. FORSTER
Executive Director, Technology Affinity Group

ENSURE THE BASICS ARE COVERED

This handbook answers the question: *What are the basic areas I should cover to improve my organization's cybersecurity? How do I get started?* Sound cybersecurity measures remain one of the most critical elements of an organization's mature risk posture. In recent years, hacking techniques have shifted from traditional perimeter breaches, to preying upon a much easier target: the unsuspecting team member.

> **Recent reports suggest that upwards of 90% of global cyber exploits were caused by successful phishing attacks.[1]**

Moreover, as the world goes mobile, so do the 'Bad Guys', or those who would seek to exploit your organizations' vulnerabilities. In 2017, 60% of fraud originated from mobile devices; of those fraud cases, 80% originated from compromised mobile apps.[2] Couple this with an organizational culture in the social sector that values transparency, openness and a trusting stance, and we see a perfect storm emerging for operational calamity and reputational risk.

So how do organizations best defend against these serious environmental factors? In our experience, we've found that a multi-pronged combination of solid policies, tools, and end-user training goes a long way in protecting an organization. Together with peers at foundations like yours, we've formulated this handbook to provide pragmatic strategies and real-world tactics based on our everyday experience as IT leaders.

In this handbook, you'll find recommendations for:

1. Security Policies
2. Training Programs
3. Best Practices and Tools

Let's get started.

[1] *"The Stealth Report", https://www.datex.ca/blog/21-terrifying-cyber-crime-statistics, October 26, 2018, accessed August 15, 2019*

[2] *Ibid.*

POLICIES

Ultimately the goal of IT policies and procedures is to maximize value to the organization – through productive use and application of products and services.[3] In a space as complex and ever-evolving as technology, senior leadership as well as rank-and-file colleagues look to IT for guidance to reduce risk. Despite reports indicating a rise in cybercrime awareness, however, people still engage in risky online behaviors:

> **Upwards of 70% of us click on links we are not 100% sure of, with millennials tipping the scales as the most affected demographic (53% experienced cybercrime in 2017).[4]**

While IT is often deemed to be overly restrictive or too "command and control" oriented, security is an area where policies can help. The two types of critical IT policies any mid-to-large sized organization should consider are Security Policies and Acceptable Use Policies.

SECURITY POLICIES

Basic security policies relate to shared computers, individual workstations, network/remote access, and data usage, as well as physical security. At a minimum, the following acceptable use policies should be in place:

- **Technology Standards Policy:** Standards related to systems implementation as well as technology purchasing, acquisition, installation, and disposal
- **Services Related Policies:** Development and delivery standards (support, maintenance, strategic planning, etc.)
- **IT Organizational Policies:** Standards that seek to identify IT mission, roles and responsibilities/structures (e.g., IT Steering Committee)

ACCEPTABLE USE POLICIES

"Acceptable Use" refers the use of hardware/software, networks, Internet/Intranet, and email. These are worthy of highlighting and separating into more focused categories. At a minimum, the following acceptable use policies should be in place:

- **Social Media Policy:** Given its ubiquity and cross-over between corporate and personal spaces, a carefully articulated policy is a must.
- **Telecommuting Policy:** Such policies establish the do's and don'ts of remote access as well as parameters for data that leaves the organization.
- **Mobile Device Agreement (BYOD):** These address the organization's stance on administrative control (e.g. remote wipe, controlled installation of apps, loss/stolen device reporting protocols, etc.).

---

[3] *"Six Keys to Sound IT Management Policy and Procedure", ITToolkit.com Magazine, https://www.ittoolkit.com/articles/planning-IT-policies, , accessed August 15, 2019*

[4] *Ibid., "The Stealth Report".*

POLICY IMPLEMENTATION

A cornerstone to the implementation of sound IT policies is **communication and education**.

IT Toolkit Magazine cites 6 keys to sound policy and procedure implementation:[5]

1. **Purposeful** to fill defined needs and serve an actual purpose.
2. **Relevant and aligned** with actual needs and matched to the intended purpose.
3. **Fully useable, actionable and capable** of implementation and enforcement.
4. **Flexible** for adaptation to reasonable variations and exceptions.
5. **Credible and fully justified and enforceable** in a consistent manner.
6. Be developed and implemented with **end-user input and buy-in**.

The concept of "enforcement" in Points 4 & 5 above is important. Given the sophistication of phishing techniques in the wild – be that through email address spoofing/impersonation, non-ASCII characters in email headers, and clever use of corporate graphics (e.g. bank fraud) – it is increasingly difficult for even the wisest end-user to avoid being duped. Reasonability must be balanced with organizational constraints such as the budget for intrusion detection systems and training that the organization has at its disposal. It may be difficult to discipline an employee if the phishing technique was highly sophisticated and your budget is small.

Ultimately, responsibility for implementation falls to senior leadership in the organization to acknowledge the risk context, indicate the tolerance the organization is willing to accept, and in turn allocate budget accordingly. These decisions help drive policy implementation and ultimately, effectiveness.

TOOLS & PRACTICES

From multi-factor authentication to physical server room security, there are many tools and practices at the IT Administrator's fingertips that are worthy of highlight. Indeed, one could write volumes on any one of these subjects. However, we have chosen key areas where we believe the small-to-mid-sized organization can move the needle within their IT operations.

PASSWORD MANAGER TOOLS

Given the ubiquity of online services that insist on online user accounts, the human mind reaches memory overload and simply cannot realistically recall credentials. This often leads to bad practices such as using the same password across multiple online services thereby increasing the likelihood a hacker can gain access to one's email, social media, and banking information. With network policies insisting staff change passwords every 60 – 90 days, workplaces continue to run up against the dreaded "post-it note on the monitor" syndrome or credentials "securely" taped beneath one's keyboard.

> **Best practices now suggest a complex *passphrase* with alpha-numeric and/or special characters making it even more difficult for the average person to keep track of myriad accounts and services. *A password manager is essential.***

[5] *Ibid, "Six Keys to Sound IT Management Policy and Procedure"*

Not only do password managers help inventory and store credentials securely, most offer some method to help users come up with secure passwords (detecting and avoiding duplicates) and even auto-launching login URLs from within the manager thereby increasing user adoption. LastPass, PassPortal, Zoho Vault, Keeper, and Dashlane are but a handful of popular tools in the marketplace but this recent PC Magazine reference compares a number of leading password manager products, including free ones.[6]

Keep in mind that an important feature for whatever tool your organization adopts is the ability to periodically export the passwords either to secondary storage for recovery or in the event that you wish to change tools and adopt a different product down the road.

CYBER INSURANCE

Given the staggering rate of cyber-attacks waged against small to medium-sized organizations per year, one of the important tools for consideration in your toolbox should be **cyber insurance**. When a cyber breach does occur, direct costs related to ransom payment(s), recovery, forensic & legal fees, regulatory reporting, and possible litigation potentially represent an existential threat to an organization's survival.[7]

> **Recent studies suggest that companies that contained a breach in less than 30 days saved $1 million USD.[8] This suggests that insurance and managing risk has a cost, but also an ROI.**

Given the relative novelty of cybersecurity coverage, insurers and underwriters are still in unfamiliar territory in understanding risk exposure, associated recovery costs, and reputational damage – making it difficult to determine what insurers will and will not pay out.[9] The importance of reading "the fine print" cannot be overemphasized. Recent events such as *NotPetya* and *WannaCry* exploits left large multinational companies on the hook for huge losses related to supply chain logistics and shipment delays after insurers deemed these attacks to be "an act of war", and therefore not covered by policy.[10] Equally, underwriters have had a difficult time determining worst-case scenarios across different sectors – especially given the relative secrecy of corporate breaches – all of which make it difficult for insurers to set premiums.[11]

When applying for cyber insurance, organizations must demonstrate their level of cyber maturity via detailed application paperwork. In other words, **insurance is no substitute for a strong resilience posture.** Evidence of solid practices helps keep annual premiums down but more importantly, could improve the likelihood of an insurance company paying out on a claim. User policies represent a solid

---

[6] *"The Best Password Managers for 2019", PCMag.com, June 27, 2019, accessed August 29, 2019, https://www.pcmag.com/roundup/300318/the-best-password-managers*

[7] *"Protect your organization from cyber crime", IBC/BAC, accessed August 20, 2019, http://www.ibc.ca/on/business/risk-management/cyber-liability*

[8] *Ibid., "The Stealth Report".*

[9] *"Cybersecurity Insurance: Read the Fine Print", TechRepublic, April 28, 2019, accessed August 25, 2019, https://www.techrepublic.com/article/cybersecurity-insurance-read-the-fine-print/*

[10] *"Cyber Insurance: A Study in Fine Print", Forbes Insights, August 14, 2019, accessed August 25, 2019, https://www.forbes.com/sites/insights-ibmresiliency/2019/08/14/cyber-insurance-a-study-in-fine-print/#57810cc82d58*

[11] *Ibid., "Cybersecurity Insurance: Read the Fine Print"*

proactive measure, but the presence of policies *evident at the time of a crisis* also reduces liability and meets the conditions that insurance companies require for coverage.

Insurers can — and will — refuse to cover events that could have been avoided.

Typically, cyber coverage tends to focus on some combination of four components:

1. Errors and omissions
2. Media liability
3. Network security
4. Privacy

Coverage can include other areas but as above, payout caps, deductibles, and premiums are all variables. These elements depend on such things as the sector within which the organization operates, annual organization income, the extent to which the organization has demonstrated a solid security posture, has retained competent internal/outsourced expertise, etc.[12]

INCIDENT RESPONSE PLAN

As described above, the indirect costs of a cyber intrusion linked to business interruption and lost employee time can be detrimental to an organization's survival. The importance of a rapid recovery framework is vital.[13] Organizations can prepare for several what-ifs by creating adequate redundancies, practicing disaster scenarios and defending critical systems, otherwise known as a solid **Incident Response Plan (IRP).** It is highly recommended that organizations engage a properly certified consultant who is well-versed in IRP methodologies and practices to lead the engagement.

The critical features of an IRP include the following steps:

1. ***Conduct a Business Impact Analysis:*** This sets a baseline from which to determine the impact of a business interruption and the key assets needed to sustain and recover all time-critical activities for each department.
2. ***Determine RTO:*** The organization needs to estimate the Recovery Time Objective (RTO). This is approximately how long the organization can sustain reasonable downtime before business operations significantly affect clientele, reputation, etc.
3. ***Develop the Business Continuity Strategy:*** The organization then develops optional strategies to mitigate and respond to a business interruption. This includes agreeing to recovery priorities, RTOs, as well as other business continuity tools and their associated costs.
4. ***Develop the Crisis Management Plan:*** This plan typically includes emergency communication protocols, system/file recovery measures, and identification of when systems should failover to a redundant data center, and whether teleworking and/or a temporary workplace location for select staff is warranted.

At a minimum, organizations should have in place a solid communications plan that considers external and internal messaging based on several key cyber breach scenarios. One does not want to be wordsmithing these messages during a crisis. Response statements should be prepared by your

[12] *Ibid.*

[13] *Ibid., "Cost of Canadian Data Breaches Continues to Rise".*

communications team or consultant and, ideally, reviewed by counsel for accuracy and legal exposure.

An IRP is ultimately a trade-off between the cost of implementing recovery methods versus potentially adverse business impacts, therefore executive participation and buy-in of the above steps is critical.

OPEN SOURCE INTELLIGENCE

So far, we've been discussing tools that respond or anticipate *potential* cybersecurity risks. This is valuable, but it would be great to know what *actual* risks the organization faces. What do the 'Bad Guys' know about weaknesses in your organization's security posture? That's where Open Source Intelligence (OSINT) comes in.

What is Open Source Intelligence? Collectively, it's a publicly available database that can be examined in a security context. It provides a way to understand what hackers can see when they look at your network. It's like checking to see that you locked the front door before you leave for the day.

One example of OSINT would be the website, https://haveibeenpwned.com/. This website examines databases of stolen email addresses to see if the address you provided is found there. The databases are publicly searchable but are easier to access through tools such as the website above.

For those who don't want to comb through OSINT datasets, we've found the service Hacker Target, recommended to us by a fellow TAG member, to be useful. Hacker Target starts with an organization's domain and checks for potential issues such as leaked email accounts on compromised databases, open DNS entries, associated IP addresses and network endpoints, and metadata associated with posted files.

Hacker Target and similar tools provide a prioritized list of remediation actions. This makes it easier to build remediation actions into your IT budget.

This last potential threat — metadata associated with posted files — is an interesting one. Foundations try to be as transparent as possible in their operations, so information like the author of a document would not normally be considered a problem. However, if the metadata includes geo-location tags associated with images of individuals, this could represent a compromise to the individual's safety.

PENETRATION TESTING

While people are your organization's first line of defense, it's vital to know your vulnerability. **Penetration testing** is an invaluable part of your toolbox that scans your network, looking for known vulnerabilities. These vulnerabilities are often machines using operating system software versions that contain known weaknesses. For instance, a web server might be running a version of Javascript that has components known to be susceptible to attack.

Penetration test tools scan your network, catalog known vulnerabilities, and provide a report that includes suggested steps to remediate the discovered vulnerabilities.

Conducting penetration testing annually is a great place to start. However, conduct penetration testing after major network changes and after any network breach.

Penetration tests are normally conducted outside your network's firewall. This mimics the actions that an attacker might take to discover and exploit weaknesses in your network. There are many penetration test tools available such as Nessus, Qualys, Netsparker, Acunetix, and OWASP; some vendors provide free or reduced-cost tools for non-profits. These tools generate a large amount of information, including a listing of vulnerabilities and a prioritization based on estimated severity. The reports can be difficult to read, so it may help to seek out a partner or consultant that can run the tests and interpret the results with you.

It's key to understand that the terms "penetration testing" and "vulnerability assessment" are often used together. However, these two are not the same.

- Penetration testing involves ***identifying vulnerabilities*** in a network and attempting to exploit them. The goal is to check whether a vulnerability really exists and to then prove that exploiting will cause damage.
- A vulnerability assessment ***aims to uncover vulnerabilities*** in a network and then recommends a mitigation/remediation to either reduce or remove the risks.

Many organizations stop at penetration testing, preferring to fix known vulnerabilities rather than determine if the vulnerability is exploitable. Making the case for one versus the other, a vulnerability assessment will help you understand the level of risk that the discovered vulnerability presents.

Whether you conduct penetration testing alone or testing along with vulnerability assessment, it's important to fix any uncovered vulnerabilities. An insurance carrier, upon learning that a security breach occurred—possibly as a result of a vulnerability that was known but not remediated—might deny the organization's security coverage claim.

For additional detail on pen testing, current TAG members are invited to watch the August 2019 webinar *How to Conduct Penetration Testing* available at: https://www.tagtech.org/page/cybersecurity.

BACKUP AND RESTORE

You may be puzzled to see backup and restore included as a security tool. We can summarize the reason in one word: **ransomware**.

In a ransomware attack, the hacker gains access to your network and encrypts files and documents stored there. Ransomware stories continue to make the news and are on the rise, most recently involving local governments in Texas, Florida and Louisiana.[14] The effect of ransomware can range from annoying (having to recover some documents) to debilitating (shutdown of the organizations' operations).

> **Paying the ransom to get your data unencrypted can be expensive. And there's no guarantee that you'll recover everything. The best approach is thorough and frequent backup of data onto storage that's not connected to the same network.**

[14] *"Ransomware Continues Assault Against Cities and Businesses", Malwarebytes Labs, Christopher Boyd, updated August 27, 2019, accessed August 30, 2019, https://blog.malwarebytes.com/ransomware/2019/08/ransomware-continues-assault-against-cities-and-businesses/*

The only caveat is that if the data is exfiltrated and finds its way into the possession of hackers threatening to expose anonymous information of your fund holders or otherwise release to the dark web, the backup scenario will not help in this situation.

It's important to run both complete and incremental backups, so that data can be quickly restored after a ransomware attack. The location of your backup can vary from tape to hard drive, solid state drive, or a cloud backup service such as AWS or Azure. Just remember that it is your responsibility to secure your data stored in the cloud. The cloud provider handles access security, but you are responsible for the recovery of your data.

Of course, the time to test your backup and restore procedures is when everything is going well and not when a ransomware attack has taken place.

Test your backup and restore procedures at least annually; every six months is even better.

There are numerous backup and restore products available including Barracuda Networks, Carbonite, Veeam, Symantec, and Egnyte. Some are premise-based, some are cloud-based, and some provide a hybrid of the two. We recommend cloud-based solutions. But some customers, concerned about the time needed to restore data from the cloud, prefer to use a hybrid solution for faster restoral. This latter choice might work for you if your Internet bandwidth is limited or if you have a lot of data to restore.

At Vancouver Foundation, the organization runs a hybrid model across different mediums. The Foundation relies heavily upon Veeam technologies for their cloud backup solution. In a true "disaster" scenario where Internet and secondary Internet connections are down, cloud backups will be inaccessible. As a secondary measure, Vancouver also backups data to an on premise NAS device and in turn runs off-site copy jobs to external hard drives on 2-week rotations (1-month restore capability). Finally, the organization runs a complete file system, SQL (including transaction logs), and AD snapshot for permanent offsite storage every 6 months. For anti-ransomware measures, VF runs file system backups every hour during the business day.

Public cloud providers like Amazon and Microsoft have backup and restore utilities that automate the process for you. Just remember, it's still critical that the backup device be separated from the rest of your network so that it's not encrypted by ransomware as well.

TRAINING

Cybersecurity is a shared responsibility. Therefore, training staff on how to recognize and react to phishing attempts is a crucial part of an organization's security. It's now understood that the most common method used to breach organizational networks is **credential theft** or stealing a user's login name/email address and password.

> **"Our staff is the best firewall we can ask for as well as our last line of defense that can never be replaced by technology. We appreciate their efforts and willingness to partner with IT Security and treat them as such."**
>
> **– Oleg Bell, Global Head of IT Security, Open Society Foundations**

As an IT leader, you have the responsibility to equip your teams with the skills to recognize and respond to phishing messages. You'll want to test their training by conducting periodic phishing tests and measuring how many recipients follow the suspicious link in the phishing message. Companies like Knowbe4, SANS, Rapid7, and Wombat Security all offer phishing simulation tools and associated training materials. These are a great place to start.

It's a good idea to reinforce that people are a central part of your security strategy. We've found that **face-to-face, customized training** is often needed to supplement training. Why?

- User engagement with training documents and videos is typically low.
- An organization's worst phishing offenders are often the people who are too busy to watch training videos.
- Tailoring security training to the organization's needs and situation increases engagement. For instance, it's possible to use actual phishing messages received by staff as examples.
- Tailored security training allows you to include information on the specific steps or procedures staff should follow when they receive a phishing message or mistakenly click on a suspicious link.

We've also found that periodic one-hour training sessions work well. These can be conducted live, or through video conferencing, and recorded for later viewing. Prizes for correct answers, demonstrations, games, and polls are all techniques that can be included to make security training more memorable and valuable. It's also helpful to mention, as a part of the training, that cybersecurity knowledge is useful for staff to protect themselves outside of work as well.

In summary, your training approach should:

- Be people-focused, ensuring all members of your team (staff and vendors) are included.
- Include regular phish-testing
- Include in-person components to ensure engagement

For additional detail on developing your approach to security awareness training, read the TAG publication "*CASE STUDY: How Our Organizations Provide Security Awareness Training*."

SUMMARY OF RECOMMENDATIONS

This document seeks to demonstrate the value of a multi-pronged approach to cybersecurity and provide you a few recommendations as a baseline. By no means are the tools and approaches described above designed to be exhaustive. These recommendations have, however, proven to be effective in enabling IT personnel to raise awareness with stakeholders about the need for an engaged staff and a multi-faceted approach.

In summary, we would like to leave you with an outline of key points, to give you a solid foundation when building your cybersecurity approach.

- **Security Policies**
  - Have an Acceptable Use policy!
  - Co-create policies with staff, for staff.
- **Best Practices and Tools**
  - Consider adopting a Password Manager as a first step.
  - Discover and assess your vulnerabilities – before a cyber-criminal does.
  - Backup – often and off-site if possible.
  - Look to Open Source Intelligence tools to see what hackers can discover about your security
  - Research Cyber Insurance as a proactive investment.
  - Develop an Incident Response Plan with your executive – their buy-in is key.
- **Training Programs**
  - An engaged and informed staff is your best defense.
  - Train staff on a regular cadence.
  - Conduct periodic phishing tests to see how well the training has worked.

RESOURCES

Below are links to the tools and resources referenced in this document.

- OSINT Training - https://www.sans.org/course/open-source-intelligence-gathering
- DIY Security - https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/#gref
- Phishing Statistics - https://www.phishingbox.com/resources/phishing-facts
- See the SANS Institute for sample information security policies - https://www.sans.org/security-resources/policies
- TechSoup (http://techsoup.org) is always a good resource for foundations and non-profits

ABOUT THE AUTHORS

DAN CALLAHAN

Vice President, Global Services
CGNET

https://www.linkedin.com/in/danielcallahan/

Dan is responsible for development of CGNET's cloud and cyber security services. He oversees all aspects of CGNET's Office 365, Teams/Skype for Business, Azure, Enterprise Mobility + Security and Dynamics CRM Online cloud services. He also oversees all aspects of CGNET's vulnerability testing, GDPR compliance, risk assessment and security consulting services. As a consultant, Dan has conducted many technology planning, security, change management and tool selection projects. Dan served as Director of Marketing and Business Operations at CGNET from 1999 to 2003. Prior to rejoining CGNET in 2011, Dan held Director- and VP-level positions in Product Management and Marketing at iPass (acquired by Parateum), SOMA Networks, Daintree Networks (acquired by GE) and YouSendIt (acquired by OpenText).

CHARLES BONAME

Director, Information Technology
Vancouver Foundation

https://www.linkedin.com/in/charles-boname-0b03b517/

Charles Boname joined Vancouver Foundation in 2014 bringing a wealth of technical expertise and project management with him from the public legal sector. Charles leads a large team of full-time & contract IT professionals to deliver stable applications and business value atop a secure computing environment.

Charles brings a disciplined yet creative voice to the table in leading change, communicating technology and achieving organizational improvement. He has strategically dedicated budget & technical resources into fortifying the Foundation's perimeter security while strengthening staff's cybersecurity awareness.

ABOUT THIS SERIES

The *CyberSecurity Essentials for Philanthropy* series launched in 2019 is provided by the Technology Affinity Group (TAG) in partnership with member organizations and private sector advisors.

View the full curriculum available for the series at: tagtech.org/cybersecurity

This is an educational publication and is not intended as legal advice. You should contact your attorney for legal advice. The opinions expressed here are the opinions of the individual authors and may not represent the opinions of their employers or of TAG.

TAG CYBERSECURITY WORKING GROUP

This work is led on a volunteer basis by the TAG Cybersecurity Working Group whose members include the following:

Jim Rutt (Chair), Dana Foundation
John Mohr, The MacArthur Foundation
Oleg Bell, Open Society Foundations
Karen Graham, Idealware
Darlene Ott, The Winnipeg Foundation
Dan Callahan, CGNET
Calvin Lewis, Cleveland Foundation
Christopher Jean-Pierre, Wellspring Philanthropic Fund
Steve Jarboe, Accenture
Anthony Putignano, Wizehive
Charles Boname, Vancouver Foundation

FUNDING PROVIDED BY

This series is funded in part through an award from the Robert Wood Johnson Foundation President's Grant Fund at the Princeton Area Community Foundation.