Connecting the Information Dots

A Webinar Series for International Not-For-Profit Organizations
# Upcoming Webinars – 2015/2016

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weds, Dec 09 @ 11:30AM – 12:45PM ET</td>
<td>Information Security &amp; Data Privacy: Why NGOs Need to Pay Attention</td>
</tr>
<tr>
<td>Tues, Jan 12 @ 11:00AM – 12:00PM ET</td>
<td>Skype for Business: Microsoft’s “New” Communications &amp; Collaboration App (a NetHope Webinar)</td>
</tr>
<tr>
<td>Tues, Feb 16 @ 11:30AM – 12:45PM ET</td>
<td>NGO Online – an Integrated Information System for NonProfits</td>
</tr>
</tbody>
</table>
Webinar Recording

• We’ll be recording the webinars in our series
• We’ll make these recordings available to those who attended the webinars first, and then to the general public
Questions

• Type your questions in the QUESTIONS box of the control panel. We’ll ask the presenters to respond to timely questions during their presentation. We’ll address the rest of the questions at the end of webinar.

• By default, your microphone is muted. Because we have so many attendees, we’ll keep everyone muted throughout the webinar.
Today’s Webinar

Information Security & Data Privacy: Why NGOs Need to Pay Attention

Presenters
Michael Duggan, Chief Information Officer, Trocaire
Joel Urbanowicz, Manager, IT Deployment Services, Catholic Relief Services.
Branko Bokan, Senior Information Security Engineer, Apextech LLC

Moderators
William Lester, Executive Director, NPOKI
Igal Rabinovich, CEO, n-Village
Marie McNamee, InsideNGO
Let’s Take a Quick Poll!

- We want to learn about your organization
- We want to learn about your organization’s Data Privacy Policy
Information Security & Data Privacy: An NGO Primer

Michael Duggan – Chief Information Officer

Joel Urbanowicz – Manager, Deployment Services
Presentation Agenda

Opening
What are we here to talk about?

Information Security
What do I need to know, and how do I start improving my resiliency?

Introduction
Presenters
Data Privacy
How do we address the Data Privacy challenge?

Collaboration
How can we leverage each other to collectively improve our maturity in InfoSec and Data Privacy?

Closing
Takeaways and Action Items
Opening

- Low to no organizational awareness on Information Security and Data Privacy/Protection in the INGO sector
- Low to no budget for Information Security and Data Privacy/Protection.
- Enormous skills gap in our community
- And yet, the need to address the security of our systems and the privacy of our data is ever increasing
- Politico/Legal compliance issues around Personally Identifiable Information (PII)
- What do we do about it?
Introduction

Michael Duggan

Michael Duggan is the Chief Information Officer at Trocaire, the Irish Catholic Agency for International Development, where he oversees the ICT strategy and operations of the organization’s global work in Africa, Asia and Central America. Outside of his work in the nonprofit sector, Michael has worked for software start-ups, energy utilities companies, government and financial services. Michael holds a Master’s degree in Business Administration from the Smurfit School of University College Dublin, a Bachelor’s of Science in Computer Science from Trinity College Dublin and a diploma in Management from University of Limerick.
Introduction

Joel Urbanowicz

Joel Urbanowicz is Manager of the Deployment Services team in the Global Knowledge and Information Management (GKIM) organization at Catholic Relief Services. He received a B.A. degree in Communications from Michigan State University and an M.S. in Information Management from Arizona State University. He has actively worked in the information technology service management and governance domain for the past 8 years at private, public, and not-for-profit institutions. His current focus is maturing CRS' global information security program and fostering collaboration between solutions and operations to ensure service quality.
Information Security Primer

The Environment
What is influencing or compelling our action in this domain?

Program Approach & Design
What are the responsibilities of this capability? What should I design against?

Quick Wins
With limited resources, how can I make a difference?
The Environment

- Increased threat to our organizations, demonstrated by recent breaches
- Existing and forthcoming donor requirements for information security
- Expanding threat surface via mobility, BYOD, consumerization of IT, etc.
Information Security Program Approach

- Information Security Oversight
  - Program Mgmt.
  - Metrics and Reporting
- IT Risk
  - Business Liaison
  - Marketing
  - Policy and Compliance
  - Third-party Security
- Security Engineering
  - Threat and Vulnerability Mgmt.
  - Risk Evaluation and Processes
- Security Operations
  - Policies and Architecture
  - Application Security
  - Infrastructure Security
  - Device Monitoring and Mgmt.
- Executive Leadership Awareness
  - Enterprise Governance, Risk, and Compliance
  - General System Development
  - System Administration
- End-User Awareness
  - Business Continuity
  - Enterprise Security Systems
  - Incident Response
- Event and Information Mgmt.
  - Integration
  - Incident Mgmt. and Forensics
- Incident Response
Information Security Design Standards

Auditable Standard
- NIST 800-53 (US)
- ISO/IEC 27001 (EU)

Actionable Guidance
- Critical Security Controls
- Risk Management
- Security Controls
- Training & Awareness
- Ongoing Monitoring

IT Fit
- Organization fit with other process areas

Information Security Program
Quick Wins

• Assign responsibility for information security
  • At minimum, give this individual equivalent access to the CIO as the development and operations heads
  • Consider moving Information Security out of IT
• Budget specifically for information security
• Shore up your security policy gaps
  • Acceptable Use, Server/Laptop/Desktop/Mobile Security, BYOD, Incident Response, etc.
  • Consult other organizations or best practice (ex. SANS) to avoid reinventing the wheel
• Focus on end-user awareness
  • Low annual investment cost (~$10 per end-user)
  • Suggest year-round training and communication program (ex. SANS Securing the Human)
• Prepare for the inevitable
  • Document and drill an incident response and breach notification process
  • Contact your insurance broker to inquire about breach insurance (will require an assessment)
  • Identity a partner to engage for worst case (ex. FireEye zero cost incident response retainer)
• Evaluate existing systems and tools to improve security
  • Use industry best practice (ex. Critical Security Controls) to guide effort...start with “Top 5”
  • CRS example: Utilized software compliance and reporting mechanism in system audit platform to identity and remediate end-user devices with Malware and PUPs
Data Privacy/Protection
The Burgeoning DP Challenge

1. Why Us & the Policy Divide
   How is data privacy policy evolving? What does it mean for us?

2. Data Privacy and Protection Guidelines
   How should we, as INGOs, approach this domain?

3. The Challenge
   What do we do to decisively respond to these challenges?
Why DP?

- Data Protection is being thrown in with Infosec despite being an entirely “new” and different capability.
- Data Protection is the **appropriate use of that data**. It applies to Personally Identifiable Information (PII).
- This creates a number of challenges:
  - Low to no organizational awareness on Data Protection (DP)
  - No resources allocated towards DP
  - EU General Data Protection Regulation a game changer for EU
  - Countries adapting DP legislation
  - Existing IT Frameworks for Infosec – ISO27001, NIST etc. but very recent for Data Protection (ISO29100)
Why us?

National Right to Information Laws, Regulations and Initiatives 2015

*Not all national laws have been implemented or are effective. See http://www.article19.org/
The Policy Divide

United States

- Privacy is often compromised for national security
- Opt-out
- Confusing federal and state-specific policy portfolio
- Definition of PII varies widely by sector

European Union

- Data Protection is a fundamental right
- Double Opt-in
- Single, all-encompassing data protection framework
- Definition of PII is well-defined
Nothing is agreed until everything is agreed!

- General Data Protection Regulation (GDPR) to be implemented Dec 2017
- Applies to organizations based outside the European Union if they process personal data of EU residents
- Fines
  - a warning in writing in cases of first and non-intentional non-compliance
  - regular periodic data protection audits
  - a fine up to 1,000,000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater (Article 79, Number 6)
- DPO Required for multinational organisations
  - Monitoring of DPOs will be the responsibility of the Regulator rather than the Board of Directors of the organisation that employs the DPO
  - Legal obligation to notify the Supervisory Authority without undue delay
- The General Data Protection Regulation (GDPR) will cost hundreds of millions to implement and billions in lost revenue src: Info Age
The Evolving Policy Landscape

• The Court of Justice of the European Union (CJEU) recently struck down the Safe Harbor agreement
  • Organizations are scrambling to respond to this development and adhere to strict data sovereignty laws in the EU

• United States is considering a new data-sharing bill (CISA) with no privacy protection
  • US government calls for regulation to mandate the provision of exceptional access mechanisms (AKA encryption backdoors)

• It is expected that the Global South will take the EU’s lead in developing data privacy policy
  • With this in mind, we must prepare our programs and organizations to comply with EU data privacy policy
Change in our Programme Countries

• Largely adopting EU type frameworks
• African Union Convention on Cyber Security and Personal Data Protection being ratified
• Complex scenario with varying legislation.
• Kenya, Madagascar, Mali, Niger, Nigeria, Tanzania, and Uganda
Donor Contracts

DFID Standard Contract – Section 30
(h) notify DFID (within two Working Days) if it receives: (i) a request from a Data Subject to have access to that person's Personal Data; or (ii) a complaint or request relating to DFID’s obligations under the Data Protection Legislation;
(l) not Process Personal Data outside the United Kingdom without the prior written consent of DFID and, where DFID consents to a transfer, to comply with: (i) the obligations of a Data Controller under the Eight Data Protection Principle set out in Schedule 1 of the Data Protection Act 1998 by providing an adequate level of protection to any Personal Data that is transferred; (ii) any reasonable instructions notified to it by DFID.
What should we do?
Core Values and User Rights

• Knowledge and Transparency
  • Users/Beneficiaries should know how ICT4D data collection systems operate
  • Users/Beneficiaries should know how and with whom personal information might be shared
  • Users/Beneficiaries should know when new information is collected and/or shared

• Agency and Control
  • Users/Beneficiaries should have to consent to data collection and sharing before any information is collected
  • Users/Beneficiaries should have the ability to access, audit, and amend their personal data
  • Users/Beneficiaries should have the ability to hold data collectors responsible for gross negligence, misuse, and/or harm resulting from data collection/sharing outside of the scope of the project
Privacy Design Principles

- To help projects uphold the rights of beneficiaries and protect their data, the following five design principles have been identified:
  - Principle 1: Address surveillance risks
  - Principle 2: Limit data collection and use
  - Principle 3: Promote and facilitate transparency
  - Principle 4: Incorporate user feedback
  - Principle 5: Assume responsibility
But before we dive in....
Three Strategic challenges for our Org’s...

1. How do we as technology functions address the technical challenges that DP creates....
   - Data residence
   - Data Life Cycle Management
   - Beneficiary processes – RTBF, Queries at scale

2. How can our Organisations effectively respect the privacy of our beneficiaries and comply with legislation while delivering effective programmes? How do we develop this capability?
And finally....

3. How do we as a sector LEAD on privacy...

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.”

The Universal Declaration of Human Rights

How can we lecture Government on Rights when we may well contravene the right to privacy of our beneficiaries....
Developing the Capability – an initiative

- A sector full of standards but....
- DP now become an Organizational Requirement
  - What organizational capabilities do we need to do this?
  - What organizational capabilities do we have to do this?
  - Where does this responsibility sit in our organizations?
- How to explain to our leadership team the capability and commitment to attain this goal?
- How do we compare in the sector? Other sectors?
- How do we explain to our supporters, donors and funders how we manage DP?
- How might we share Capabilities across INGO’s?
Proposal – Baseline + Develop a Plan

Research Institute founded by Intel

Framework to demonstrate business value of IT

Data Protection Critical Capability

One of thirty seven Capabilities

More: http://dp.ivi.ie/
Deliverables

Your Agency
Deep Analysis of Maturity Levels of 11 DP building blocks for your Organisation
Recommendations & Observations

Peer Group
Benchmark Report

Stakeholders
Original NetHope Research Report for Donors and Sector Stakeholders
What we hope to achieve

• A benchmark of where the sector is currently.
• A structured understanding of where the sector needs to achieve.
• An understanding of what capabilities the sector needs to have to attain this.
• An understanding of how the sector can collaborate on this topic from a capacity building perspective.
• A method of communicating this to all stakeholders, internally and externally to establish the funds and resources to deliver an adequate DP capability in our organisations.
Take-aways

Information Security
• There are real, observed threats for NGOs
• Best practices exist to help guide our limited spend
• There quick, inexpensive opportunities to improve your resiliency

DP
• We are moving from unregulated sector to a heavily regulated sector.
• DP is an organization wide capability that must be addressed Org wide
• While IT hold the data it’s the rest of the organization that decides on what is captured and how it is used.
• We need to understand what capability our organizations need to have in order to effectively manage DP.
• We need to start a conversation on funding this capability.
Information Security for NGOs: QUICK WINS

Branko S. Bokan, CISSP, CAP, PMP
Director, Cyber Security
ApextechLLC.com
Wednesday, December 9, 2015
CRITICAL SECURITY CONTROLS

Compiled by a consortium of more than 100 experts from private and public sector. Part of a larger effort housed at the Center for Strategic and International Studies.
QUICK WIN #1

USER MANAGEMENT

Do you know your system administrators? Do you know who determines who has access to what assets and why? Do you actively manage user accounts?
QUICK WIN #2: TRAINING AND SKILLS ASSESSMENT

Overall security of any organization is only as good as the weakest link in the entire process. Frequently neglected, the end-users play a critical role in organizational security. Strong cyber defense starts with your key asset: people.
Why Training

- Clicking on phishing emails (more than 2/3 of incidents)
- User errors (sensitive information sent to incorrect recipients 30%, publishing non public data 17%, insecure disposal of sensitive data 12%)
- Privilege misuse – AKA, the “Insider Threat”
- Physical theft / loss
Training (Ineffective)  
- Off the shelf compliance-based  
- Not mandatory  
- Too technical  

Training (How)  
- Interactive  
- Customized to your needs  
- Scenario-based examples  

Training (Who)  
- Everyone  
- Start with C level  
- Involve HR and legal
QUICK WIN #3

Vulnerability & Patch Management, Malware Defenses

New vulnerabilities in software and hardware running on your network are discovered daily, sometimes even hourly. Constant monitoring and proper remediation and mitigation are key for safe operations of your IT infrastructure.
QUICK WIN #4
Inventories
Accurate inventories of both software and hardware allow for proper maintenance, backup and cyber hygiene.
QUICK WIN #5
Application Software Security
Cyber security attacks frequently come through web based applications. Application developers are rarely properly trained in secure coding and are not in the security business; their job is to get the code working.
QUICK WIN #6
Data protection and recovery
According to a study from Price Waterhouse Coopers, 70 percent of small firms that experience a major data loss go out of business within a year.
QUICK WIN #7

Secure Configurations and Network Engineering

• Do you enforce secure configurations on assets connecting to your networks?
• Do you limit and control network ports, protocols and services?
• Do you know your boundaries?
• Is your computer network engineered in a secure manner?
QUICK WIN #8

Wireless Access Control

Your employees love them. Unfortunately, so do the bad guys. Wireless networks allow them to access your resources without even being physically connected to your premises. Proper management, control and monitoring of wireless networks are key for having full control over your infrastructure.
QUICK WIN #9
Audit Logs

Deficiencies in security logging and analysis allow attackers to go unnoticed indefinitely and the particular damages done may be irreversible.
QUICK WIN #10
Incident Response

Even the best security practices cannot completely eliminate the possibility of a cybersecurity incident. When such incidents occur, the reputation of your organization is at stake and it’s too late to plan your next move.
CRITICAL SECURITY CONTROLS
Available as a checklist for evaluation and awareness of cybersecurity issues your organization might have missed:

http://apextechllc.com/cybersecurity-checklist/
Q & A
### Contact Information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael Duggan:</td>
<td><a href="mailto:michael.duggan@trocaire.org">michael.duggan@trocaire.org</a></td>
</tr>
<tr>
<td>Joel Urbanowicz:</td>
<td><a href="mailto:Joel.Urbanowicz@CRS.org">Joel.Urbanowicz@CRS.org</a></td>
</tr>
<tr>
<td>Branko Bokan:</td>
<td><a href="mailto:bbokan@apextechllc.com">bbokan@apextechllc.com</a></td>
</tr>
</tbody>
</table>
Connecting the Information Dots

A Webinar Series for International Not-For-Profit Organizations