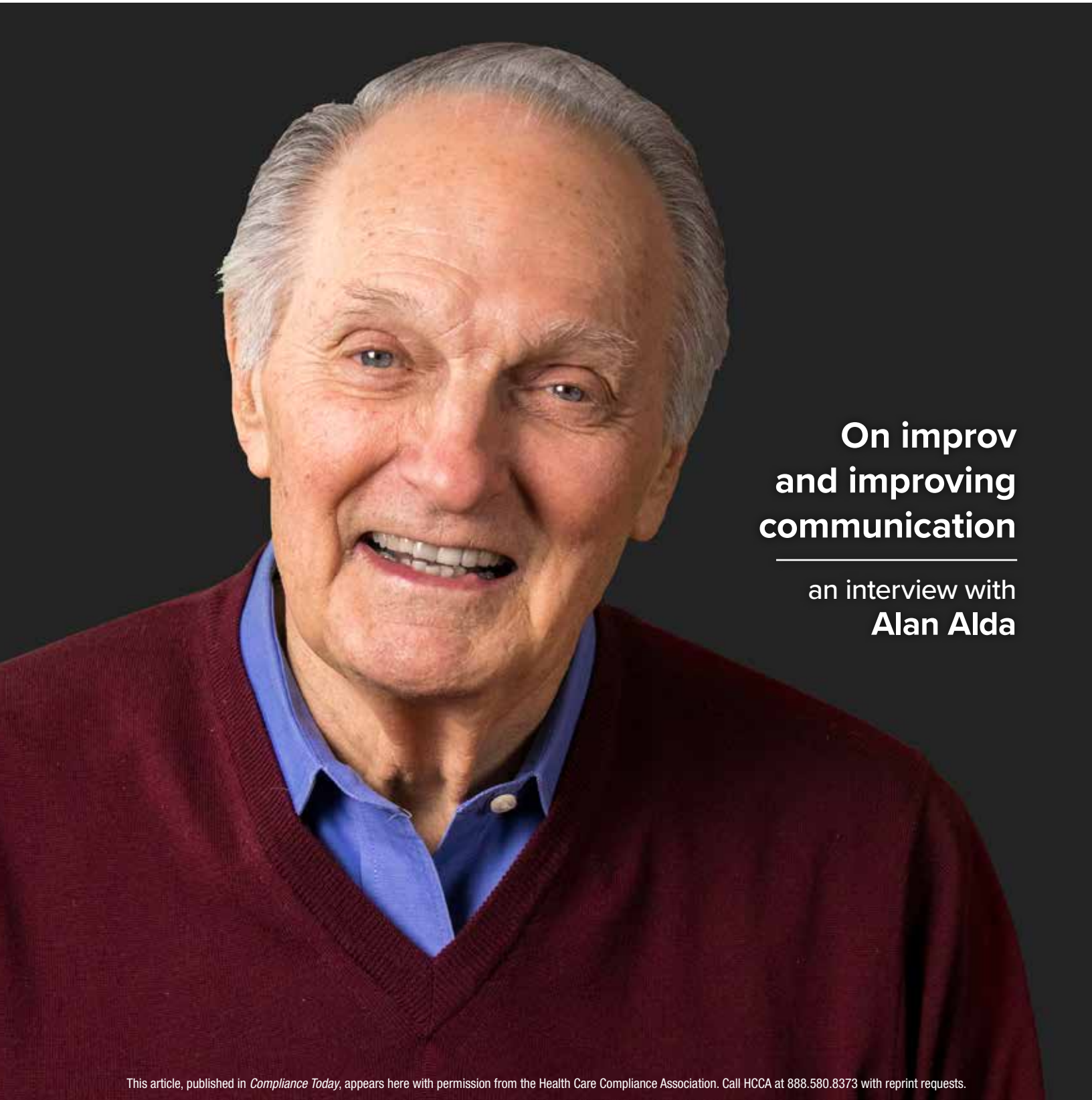
HCCA
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

MARCH 2018



On improv and improving communication

an interview with
Alan Alda

by Eric Hummel, MS CS, InfoSec

Building a security program: It's not just IT

» Executive leadership must be invested in the security program.
» Create a security program led by a compliance officer who has been trained in cybersecurity.
» Build the governance structure first.
» Propose a realistic budget.
» The security program consists of a set of projects led by domain leaders (HR, Facilities, IT, Administration, Clinical, etc.).

Eric Hummel *(eric.hummel@qipsolutions.com) is Chief Technology Officer at QI Partners, LLC in Rockville, MD.*

As the saying goes, "To a hammer, all problems look like a nail." Most healthcare companies start their Health Insurance Portability and Accountability Act (HIPAA) security program by assigning responsibility and accountability to a manager of Information Technology (IT). This creates a bias within the organization that security compliance is an IT issue. In reality, much of security does not directly involve IT. The result is that non-IT risk gets overlooked, and the IT team takes on a security enforcement duty that is both uncomfortable and ineffective.


Hummel

The need for security compliance is *not* going away. It is rapidly taking on increased importance in all organizations. Losses are starting to become significant and threats are increasing. Security is an ongoing requirement for all organizations in the 21st century. A security program needs to be built for efficiency and longevity. It needs to manage risk in a way that also meets the compliance requirements of HIPAA and state laws. This makes the choice of an organizing principle for your security program much more important.

Managing risk

Merging the twin requirements of HIPAA compliance and the need to manage risk in medium or small healthcare organizations is challenging at best. The compliance side demands that a thoroughly documented program be in place that meets certain minimum requirements. The risk side of security needs to meet the real threats of ransomware and data breaches that harm reputation and bottom line. In many communities, expertise is neither affordable nor available to plan and lead in this complex situation. But, these are compatible requirements, particularly when managed as a single program.

Left searching for cost-effective options, organizations reflexively turn to their IT staff, assigning the Chief Information Officer (CIO) or an IT manager the new responsibility for security compliance. This person is proficient in technology and possibly technical data security, but they are rarely experienced in organizational risk management. Beyond having the added burden of planning, execution, and continuous monitoring of risk and compliance, they also must lead a program that encompasses workflows throughout the

organization. Internal IT professionals should be focused on ensuring complex security aspects such as data loss prevention or security event and incident monitoring. However, things like business associate agreements and better staff background checks will likely be out of their experience range. Even though cybersecurity may seem like an IT issue on the surface, security compliance is process oriented, and risks come from all directions, not just IT.

Security is a risk management process, not an IT function. Like other business or medical risks, security should be viewed as a process to minimize potential losses by controlling sources of risk. IT is one source of risk, but there are many others that may be more important:

- Human error is a major source of risk that IT may be poorly suited to address.
- The physical layout and security features of a clinic can help or hinder security.
- Effective staff training is both needed and key to reducing human error.
- Clinical and operations staff are key stakeholders and have vast knowledge that is needed when planning for disaster or emergency operations.

These are all functions of security risk management.

Ultimately, all of these risks, whether IT, HR, clinical, financial, legal, or administrative, should be the concern of the entire organization (see sidebar).

If planned correctly, compliance will be the natural result of a comprehensive security program led by someone who understands both the risk management methodology required for security and the HIPAA compliance documentation requirements.

What is the best strategy and who should lead?

First and foremost, support for security must come from executive leadership. Security involves resources and time. Understanding business risk is in executive management's domain. Compliance is also a business risk. Merging these two risk objectives makes sense if the resulting program is managed for both. Managing them separately is a recipe for frustration and disaster. Setting up a process for assessing and reporting risk and compliance to the C-level leaders permits them to make intelligent allocation of resources and realistic expectations of schedule. Their full-throated support is a key factor for success.

One should look at security and HIPAA compliance as a series of ongoing projects that need to be managed. Individual projects, such as security training, business associate contracts, or encryption, can be assigned to the appropriate lead, but the overall strategy for controlling business risk should remain with executive leaders who are good at motivating, guiding, and measuring projects. Identifying and training the leader who will understand both HIPAA and security risk is key to keeping a single program. The logical choice for this role in a smaller organization is the compliance officer.

Security Stakeholders

Executive management
Administrative operations
Clinical staff
Human Resources
Information Technology
Physical Plant
Finance
Risk and Compliance

Risk: From threat to loss

In the language of cybersecurity, "risk" is the expected "loss" due to materialized "threats." Where threats meet "vulnerabilities," an "impact" can occur, resulting in loss. Losses are most easily quantified in terms of dollars, but other values are relevant in healthcare.

The security program must identify threats and vulnerabilities, then develop security controls that close or mitigate the vulnerabilities. Controls can also be used to limit the impact of materialized threats and to minimize the ultimate loss (see figure 1).

Compliance, governance, and risk

Security projects come in all different sizes with various objectives. The first project for an organization with very little security experience is to build security governance. Policies, roles, responsibilities, documentation, and the decision-making process are the core of governance. Much of this can be accomplished quickly and is essential to the rest of the program.

Having a good decision-making process is useless without good information to inform decisions, and this fits neatly with compliance. One of the first jobs of the new governance program is to identify the information that is needed for anticipated decisions. Baseline data about your organization should be available. How many staff? How are they trained? How many devices? What data is "business critical"? Where is it stored? Is it backed up? What is shared with business associates? What are their security practices? By delegating responsibility for accurate information to those who are already engaged in a business domain (e.g., HR, Finance, or IT), the load is spread out, and the data may be easier to collect. This is also the time for planning the collection of compliance documentation.

A good security organization structure is critical. We advise organizations of all sizes to have a security team or committee led by an executive and staffed by the leads of each business domain. It should be tasked with:

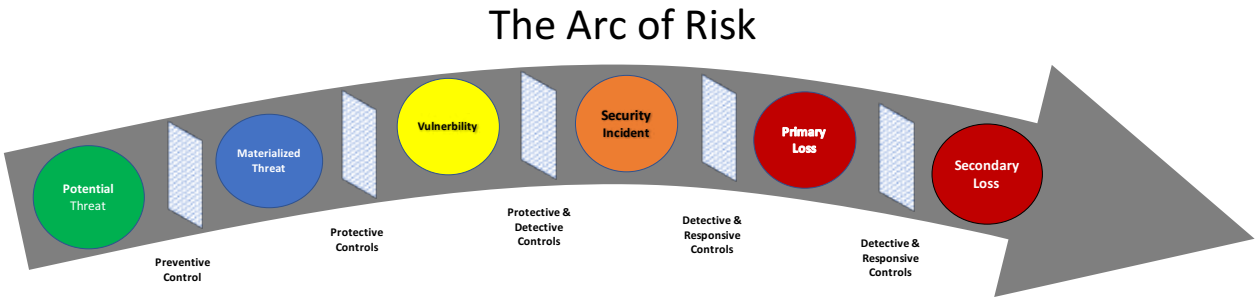
- creating, maintaining, and documenting the security program;
- ensuring that significant risks to the business are identified and understood;
- requesting and justifying a budget for security;
- assigning responsibility for projects and tracking execution;
- reporting progress on risk minimization; and
- preparing the organization to respond to security incidents and breaches of patient privacy.

The business domain leaders should be responsible for:

- collecting the necessary inventory and compliance documentation specific to their domain;
- leading the security projects that are within their domain; and
- delegating work to staff where appropriate.

Once organized, the starting point for the program should be to convene the security

Figure 1: The Arc of Risk



team to execute a startup process in roughly this order:

1. Assess the current state of security in the organization
2. Understand the legal requirements that must be met
3. Adopt organizational policies for security and privacy
4. Assign roles and responsibilities for security
5. Document a policy enforcement process
6. Circulate and train staff on security policies
7. Assess risk and prioritize security projects
8. Assign responsibility for project to business domain staff
9. Track progress of projects

Full toolbox

Effective information security requires you to use all the tools in the shed, not just the hammer. Instead of making security a responsibility of one business domain, management of the security program needs to be distributed across the organization and led from the top. Breaking down the responsibility for controlling risk to smaller projects spreads out the effort and engages staff in security. A natural outcome of the process described is continuous improvement of the security program and the capacity to control threats as they increase. Having everyone aware and participating will be the future norm as cyber threats become ever more prevalent. The result will be 360-degree visibility and the integration of security into all business domains.