ERASMUS Final Report

08.5 Discussion Section on Community Feedback

ER draft as of 07.04.17

To understand the organizational needs, specific pain points, and overall challenges of the first responder community with regard to digital identity, we interviewed a sample of experts -- members of the first responder community. The goal here was qualitative -- to identify common themes and issues that could be probed and surveyed further. See Appendix A for First Responder Interview Protocol. We interviewed:

|  |  |
| --- | --- |
| Director | EMS Services |
| Coordinator | Emergency Management |
| Deputy Fire Marshal | Fire Marshal's Office |
| IT Services | (Large State) Commission for Environmental Quality |
| Maritime Disaster Response | United States Coast Guard (retired) |

A pattern of themes emerged around the following issues:

* Security. *“I’m always worried. It’s a best effort on our end. What we use it’s a private AT&T cloud. Everything is routed back into my CISCO system.” (DS)*
* Issuing of badges*. “Problem with badge is the physical aspects. Your badge is everything — physical identity is tied to that...how does it expire. Once you lose it, you have to order. And what happened to the others?” (DS)*
* Updating credentials. *“There’s a big hole. There’s [no other option] out there — a credential reset take a long time. Can’t lose it. What makes it real? No one is storing those credentials in a centralized place. If they lost it - revoke it, reissue it, doesn’t exist.” (DS)*
* Lack of standards-- As David Smith explained: *“If there is no push to adopt the standard, it won’t happen…it has to be put out at a federal level. Right now there’s no common standard for third parties to write to that standard.”*
* Decentralization - *“Applications are out there, they are just not tied together. At some point there has to be some agreement, this is what they have to meet. I don’t see another solution. There needs to be a standard — a federal standard.”*
* Adoption Barriers
  + 1. Culture – local jurisdictions are territorial
    2. Source of directive – local jurisdictions have authority

Conclusion

The consequences of a fragmented and outdated system are highly problematic for the first responder themselves as well for the entire emergency community. There are, as one first responder said, “No other options out there.” The lack of a solution puts at risk the safety, security, and accessibility to first responders who are qualified.

Those we interviewed explained that while manual practices may be familiar and reliable, they are inaccurate, inefficient, inaccessible, and not secure. In a crisis situation accompanied by chaos and threat, these manual system of t-cards, passport systems, sign in rosters, and smart cards are wholly inadequate for confirming the essential details about an emergency responder, namely their skills, credentials, and authorizations.

Most agreed that while the mobile device offers the kind of features and functions that would be helpful in an event, the dependency on cellular network makes it unreliable. However, there are key areas where mobile technology provides a much needed solution. The areas where mobile technology would be most useful are:

* Before an event in the collecting and updating of information
* Immediately after an event, when power is restored, and immediate accounting for people and resources is needed; and
* After some extended period of time has passed and financial accountability is necessary for individuals and organizations that are billing for time and materials.

Interviewees agreed that buy-in would be biggest barrier and that an approach where DHS would set a condition for grant monies, compliance with standards, could be effective as an adoption strategy.

**APPENDIX A**

**Interview Questions**

I. INTRODUCTION

"We are gathering background information to understand digital identity in emergency responder community. We want to find out how different organizations are approaching digital identity”

1. What kinds of digital and in person credentials FR's are using.
2. What kinds of websites and mobile applications FR's are using for work.
3. C) How much friction exists accessing digital resources.

II. QUESTIONS FOR END USER

The first few questions are contextual, so we better understand the information you're sharing:

1. Person / Organization

* Tell us about the purpose of your organization?
* What is your role?
* What is the size and structure of your organization?

2. IT staff:

* Is there a dedicated IT staff?
* Is there IT staff dedicated to user and access management?

III. QUESTIONS FOR IT STAFF PERSON WHO IS RESPONSIBLE FOR USER MGT

1. Tell us about identity practices?

1. In rough terms, how many usernames and passwords (or other types of authentication) do you have? What are some of the systems people need to access? Does your organization have a single sign-on system that provides access to multiple websites?
2. (IT Question) Do you know where the organization stores usernames and passwords?

* Microsoft Active Directory
* SaaS Identity Provider (Okta, OneLogin, Microsoft Azure, Google,
* Salesforce, other SaaS)
* Other LDAP (Sun, Oracle, IBM, CA, OpenLDAP)
* Relational database (MySQL, Postgress, Oracle, MS SQL)
* Other: please explain \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. When responding to a large, multi-jurisdictional disaster, can you share your thoughts or concerns about the process for identifying people either in person, or when they use certain digital tools (mobile applications, websites)?
   1. Does the first responder have a smart card that complies with federal standards? Can you share your thoughts on these credentials?
   2. Do you think usage should be extended to more people? What are some of the challenges for issuing more smart cards (or using them)?
   3. What would you think about a mobile identity card for first responders?
   4. Do you think people in your organization would object to using to using their person smart phone to apply for a first responder mobile identity card?
   5. Are there standard certifications that you think would be important to convey via the mobile identity card? Is interoperability an issue?
   6. Can you share your thoughts about using credentials other then passwords (or smartcards) to access websites or mobile applications?
2. What are the most important organizational applications that your organization sees the need to upgrade within the next five years?