TO UPGRADE OR NOT:
THE PHYSICAL ACCESS CONTROL DILEMMA

HID Global surveyed security system users, integrators, installers, product distributors and consultants to understand their views on change and industry best practices for physical access control. Here's what we found.

MARKETS INCLUDE

- Educational institutions
- Financial service companies
- Government agencies
- Defense/Military
- Healthcare organizations
- Small/medium/large business enterprises

ARE WE KEEPING UP WITH THE BAD GUYS?

INFREQUENT TESTING

Only 37% of users perform annual security assessments.

NO THIRD PARTY TESTING

Most users do not contract a third party to test their existing physical access control systems, either through security audits or penetration exercises. This means that users either run their own test internally, or do not test.

UPGRADES

MORE THAN **50%**

have not upgraded in the last year.

MORE THAN **20%**

have not upgraded in the last 3 years.

TECHNOLOGIES

Over 75% of end-users said, cards with cryptography were "IMPORTANT" or "VERY IMPORTANT."

However, the majority believe Magstripe and Prox provide ADEQUATE SECURITY.

PERCEPTION **GAP**

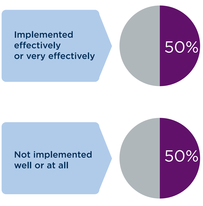
This may be a case of respondents simply not knowing how secure smart card technology can be, while overestimating the security from Magstripe and Prox technologies.

BEST PRACTICES – TECHNOLOGY

Technologies with the highest security include contactless cards with cryptography, multi-factor authentication readers, multi-tech cards and readers with OTP and PKI, and the use of a single credential for physical and logical access.

Yet while 75% felt these technologies were considered important or very important, a far lower percentage felt they were being implemented well.

IMPLEMENTATION EFFECTIVENESS:

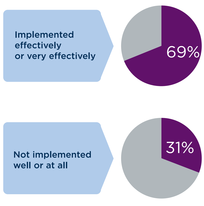


BEST PRACTICES – POLICIES

Policies with the highest security include user education, strict temporary card procedures, immediately voiding lost or stolen cards, and BYOD procedures.

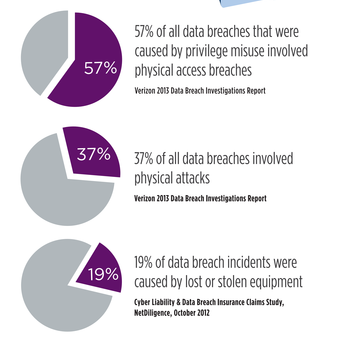
Yet while 93% felt these policies were considered important or very important, a far lower percentage felt they were being implemented well.

IMPLEMENTATION EFFECTIVENESS:



Security integrators and users believe that their security system is neither spectacular nor deficient— It is just **ADEQUATE**.

COMPLACENCY CAN BE DANGEROUS



57% of all data breaches that were caused by privilege misuse involved physical access breaches

Verizon 2013 Data Breach Investigations Report

37% of all data breaches involved physical attacks

Verizon 2013 Data Breach Investigations Report

19% of data breach incidents were caused by lost or stolen equipment

Cyber Liability & Data Breach Insurance Claims Study, NetDiligence, October 2012

THE BIGGEST BARRIERS TO BEST PRACTICES—MONEY

- Lack of budget
- Management not seeing the value
- Lack of resources and experience to implement

However, the cost of not investing in best practices can be very high:

$600,000/HOUR

Estimated cost of airport terminal shutdown after unresolved physical security breach

$5.4 MILLION

Total cost of data breach incident in 2012

2013 Cost of Data Breach Study, Ponemon Institute

That's why users and providers have to take into consideration how much money and time will be spent on the security system versus how much money they could lose after a data breach.

THE FUTURE IS NOW

- Mobile access control on smartphones will enable a more hassle-free security experience for users, who can carry all of their keys and credentials on a device they carefully protect and rarely lose or forget.
- This is a game-changing evolution with implications for both corporate security and user privacy that will fuel even more need for strong adherence to best practices.
- If the industry can't shore up its best practices now against today's threats to traditional cards and readers, the infrastructure will be even more stressed when users move to digital credentials carried on smartphones in a BYOD deployment environment that will be subjected to new and different threats.
- Technology advances continue to skyrocket as threats become more sophisticated. Legacy proprietary infrastructure, technology and mindsets make it hard to keep up.
- Migration to open technologies enables organizations to upgrade to improved security and capabilities while preserving earlier investments.

hidglobal.com

2018-08-01-hid-pacs-upgrade-or-not-ig-en PLT-04009