



CRAIG BRUCE
SECURITY TECHNOLOGY EXECUTIVE

25 QUESTIONS TO ASK BEFORE MODERNIZING PHYSICAL SECURITY

A Practical Discovery Guide
for Complex Security
Environments

Good security design
starts with discovery.
Technology follows.

CRAIG BRUCE

Security Technology Executive



START WITH DISCOVERY

Physical security modernization often starts in the wrong place.

The conversation jumps to cameras, access control, cloud architecture, manufacturers and features before the project team has fully defined the problem.

I take a different approach.

Before designing the technology, I want to understand why the organization is looking at the project now, what it is trying to achieve, how the current environment operates, what infrastructure already exists, where the hidden dependencies are, what risks matter most and how the organization expects to change over time.

The questions in this guide are 25 selected questions from a much larger discovery framework I have developed for complex physical security environments. They are not intended to replace a full assessment.

Good security design starts with discovery.
Technology follows.

HOW TO USE THIS GUIDE

These are not 25 yes/no questions to race through. They are conversation starters designed to uncover requirements, assumptions, dependencies, ownership and risk. Use them to guide discovery meetings, challenge inherited assumptions and identify the issues that should be understood before technology decisions are made.

1	Start With the Business Problem	2	Understand the Infrastructure
3	Find the Hidden Dependencies	4	Design Around How People Actually Work
5	Plan the Migration Before You Start It		

1

Why are you looking at this project now?



WHY NOW

The trigger gives context for every decision that follows.



ALIGN FIRST

Start with the business driver, not the product.

Why I Ask It

Something usually triggered the conversation. Maybe the existing system has become unreliable. Maybe there has been an incident. Maybe the organization is expanding. Maybe infrastructure is aging, support is becoming difficult or the existing environment simply no longer fits the way the organization operates.

I want to understand why now before we start talking about products. That context helps explain what is driving the project and what the organization actually needs to accomplish. From there, I want to understand the top technology and security objectives and what success should look like.

DISCOVERY NOTE

Something usually triggered the conversation.

2

What are the biggest problems with the existing system?



FIND THE CAUSE

A hardware complaint may only be the symptom.



DEFINE BETTER

Describe what must improve before comparing solutions.

Why I Ask It

One thing I have learned is not to confuse the symptom with the problem. A customer may initially believe the issue is cameras, access control or aging hardware.

After asking a few more questions, the real problem may turn out to be how people access information, investigate incidents, manage users, maintain the environment or work across multiple disconnected systems. Modernization should solve actual problems - not simply replace old technology with newer technology.

KEY PRINCIPLE

If we cannot clearly describe what needs to improve, it becomes difficult to judge whether a proposed solution is actually better.

3

What does the current system do well that you do not want to lose?



PRESERVE VALUE

Modernization should not erase workflows that already work.



ASK USERS

Operators know which capabilities they depend on every day.

Why I Ask It

Discovery should not only focus on what is broken. Every existing environment usually has something that works well for the people using it. That may be a workflow, an integration, a capability or simply something operators depend on every day.

A modernization project should understand those strengths before replacing them accidentally.

KEY PRINCIPLE

The goal is improvement - not change for the sake of change.

4

What capabilities are missing today, and what do you wish the new system could do?



LOOK FORWARD

Future-state needs can matter as much as today's pain points.



DEFINE SUCCESS

Ask what the organization wishes it could do.

Why I Ask It

Pain points tell us what is not working. This question tells us where the organization wants to go.

I want to understand what users, operators and stakeholders wish they could accomplish that the current environment does not allow them to do effectively. Those future-state requirements can be just as important as the problems we are solving today.

DISCOVERY NOTE

Pain points tell us what is not working.

5

If we changed nothing, what is the biggest risk over the next 12-24 months?



RISK OF DELAY

Doing nothing is still a decision with consequences.



SET PRIORITY

Use risk to help shape scope and sequencing.

Why I Ask It

This moves the conversation away from equipment and toward business and operational risk. Sometimes the greatest driver for modernization is not a missing feature. It is what happens if the organization continues operating the current environment for another year or two.

Understanding the risk of doing nothing helps establish priorities and gives the project team another important factor to consider when defining scope and sequencing.

DISCOVERY NOTE

This moves the conversation away from equipment and toward business and operational risk.

6

What existing infrastructure can we use?

**START WITH REALITY**

The existing environment shapes cost, schedule and complexity.

**REUSE CAREFULLY**

Some infrastructure may be suitable for continued use.

Why I Ask It

A modernization project does not start with a blank sheet of paper. There may already be cameras, cabling, fiber, switches, power, door hardware, access-control infrastructure and other systems in place.

Some of it may be perfectly suitable for continued use. Understanding what can potentially be reused can materially affect scope, schedule, cost and project complexity.

DISCOVERY NOTE

A modernization project does not start with a blank sheet of paper.

7

What infrastructure should be replaced?

**DON'T ASSUME**

Reuse and replacement are separate decisions.

**STANDARDIZE**

Modernization can be a chance to remove weak or inconsistent infrastructure.

Why I Ask It

Reuse is only half of the conversation. There may be infrastructure that the organization specifically wants removed, upgraded or standardized as part of the project.

I like to look at reuse and replacement separately because they answer different questions.

KEY PRINCIPLE

One asks: What can stay? The other asks: What should change?

8

Who accepts the risk associated with reused infrastructure?



OWN THE RISK

Existing and usable are not always the same thing.



MAKE IT EXPLICIT

Reuse should be a conscious decision with clear ownership.

Why I Ask It

This is one of the questions I consider especially important. Existing infrastructure may be perfectly serviceable, but if it was not installed, tested or documented as part of the new project, the team needs to understand what assumptions are being made about its condition and performance.

Reuse may absolutely be the right decision. But it should be a conscious decision with clear ownership - not an assumption.

KEY PRINCIPLE

"Existing" and "usable" are not always the same thing.

9

Will the security systems operate on the enterprise network or on a dedicated security network?



ARCHITECTURE FIRST

Network placement affects support, security and ownership.



INVOLVE IT

Make the network decision before deployment begins.

Why I Ask It

Modern physical security systems depend heavily on network infrastructure. Where those systems live affects architecture, ownership, support, troubleshooting, cybersecurity requirements and the teams that need to be involved.

This is not something I want discovered halfway through a deployment. It is a core architecture decision that should be understood early.

DISCOVERY NOTE

Modern physical security systems depend heavily on network infrastructure.

10

Can the existing network, fiber and PoE infrastructure support the new devices, or will upgrades be required?



CHECK CAPACITY

New devices may demand more power or bandwidth.



LOOK BELOW THE DEVICE

A camera project can become an infrastructure project.

Why I Ask It

The visible device is only part of the system. A new camera may require more power, bandwidth or network capability than the device it replaces.

Network design, switch capacity, fiber, redundancy and connectivity can all affect how reliable and supportable the finished system will be. That means a project that looks like a camera upgrade can quickly become an infrastructure project.

KEY PRINCIPLE

I want to understand those dependencies before equipment starts arriving onsite.

11

If I unplug the existing system tomorrow, what else stops working?



MAP DEPENDENCIES

Hidden integrations often surface during migration.



BREAK NOTHING

Find what depends on the system before disconnecting it.

Why I Ask It

This is one of my favorite discovery questions because it often changes the conversation. Complex environments develop dependencies over time, and not all of them are obvious.

A security platform may be interacting with systems that appear unrelated until something gets disconnected.

KEY PRINCIPLE

Find those dependencies before the migration finds them for you.

12

Which identity systems - HR, Active Directory or others - integrate with access control?



FOLLOW IDENTITY

The badge may be only the visible part of the process.



TRACE OWNERSHIP

Understand where users originate and how they are provisioned.

Why I Ask It

Access control is frequently connected to a larger identity-management process. The badge may be the visible part, but behind it may be HR systems, directories, provisioning workflows, single sign-on or other sources of identity information.

Before changing access control, I want to understand where identities originate, how they move through the organization and what other systems depend on that process.

DISCOVERY NOTE

Access control is frequently connected to a larger identity-management process.

13

What functions depend on the integration between access control and video?



ASK WHAT IT DOES

An integration matters only if a workflow depends on it.



FOCUS ON USE

Operational value matters more than an integration checkbox.

Why I Ask It

It is easy to say two systems are integrated. I care much more about what that integration actually does.

Does it help operators investigate events? Does video appear in context with an access event? Does the integration support a workflow people rely on every day? Knowing the operational dependency matters more than simply knowing an integration exists.

DISCOVERY NOTE

It is easy to say two systems are integrated.

14

What other operational systems depend on or integrate with the security environment?



LOOK SIDeways

Security platforms rarely operate in isolation.



MAP THE ECOSYSTEM

Identify systems that send, receive or depend on security data.

Why I Ask It

Physical security rarely exists in isolation. Depending on the environment, integrations might involve intrusion systems, intercoms, fire alarm interfaces, elevators, parking, license plate recognition, visitor management, turnstiles, mass notification, mobile applications or public-safety workflows.

Not every organization will have all of these. The point is to identify what does exist and understand what depends on what before anything is changed.

DISCOVERY NOTE

Physical security rarely exists in isolation.

15

Which integrations would materially improve response time or reduce operational friction?



REDUCE FRICTION

Not every possible integration is worth implementing.



VALUE FIRST

Prioritize connections that improve response or reduce manual work.

Why I Ask It

A long integration list looks impressive on a feature sheet. That does not mean every integration creates operational value.

I want to know which connections actually help operators understand an event, find relevant information, reduce manual steps or respond faster.

KEY PRINCIPLE

The goal is not integration for integration's sake. The goal is better operations.

16

What takes your operators too long to accomplish today?



WATCH WORKAROUNDS

Workarounds are clues that the system is driving the process.



FOLLOW THE OPERATOR

Daily friction should influence system requirements.

Why I Ask It

Physical security technology ultimately exists to help people monitor, investigate and respond. If an investigation requires navigating multiple systems, manually matching timestamps or searching through disconnected information, that friction should influence the design of the new environment.

When people develop workarounds for things that should be simple, I want to understand why.

KEY PRINCIPLE

Operator workflow is often a better guide to system requirements than a manufacturer's feature list.

17

Where are your biggest security blind spots today?



BLIND SPOTS ARE BROAD

A blind spot may be process, staffing or technology.



ASK WHERE IT HURTS

Find where the organization feels least prepared.

Why I Ask It

A blind spot is not necessarily a place without a camera. It may involve staffing, process, access control, perimeter coverage, communications, information availability or technology.

That is why I treat this differently from a simple camera-coverage question. I want to know where the organization feels least informed, least prepared or least capable of responding effectively.

DISCOVERY NOTE

A blind spot is not necessarily a place without a camera.

18

Where are the current camera coverage or image-quality gaps?



CHALLENGE INHERITANCE

New devices do not have to go where old ones were.



DESIGN FOR THE VIEW

Start with what the organization needs to see.

Why I Ask It

This gets more specific. Where is video missing? Where does video exist but fail to provide the detail the organization needs?

A modernization project is an opportunity to challenge inherited camera locations instead of automatically installing a new camera exactly where the old one was mounted.

KEY PRINCIPLE

The question should be: What does the organization need to see? Not: Where was the previous camera?

19

What areas are most critical during your highest-demand operations?



PLAN FOR PRESSURE

The hardest operating period exposes weak assumptions.



DESIGN FOR PEAK

Do not optimize only for the average day.

Why I Ask It

Every environment has a hardest day. For a stadium, that may be event day. For another organization, it could be shift change, peak occupancy, a major public event, a high-security operation or another period when normal conditions change dramatically.

I do not want to design only for the average day.

KEY PRINCIPLE

Design for the hardest day, not just the average day.

20

Where will the organization be in three to five years?



THINK AHEAD

Today's perfect solution can become tomorrow's constraint.



DESIGN TO EVOLVE

Consider sites, growth, acquisitions and changing use.

Why I Ask It

I am not only designing around today's requirements. Is the organization adding locations? Acquiring businesses? Growing headcount? Changing the way facilities are used? Expanding into new markets?

A solution that fits perfectly today can become the wrong solution surprisingly quickly if we do not understand where the organization is heading.

KEY PRINCIPLE

Modernization should solve today's problems without creating tomorrow's limitations.

21

What can absolutely never go offline?



UPTIME IS A REQUIREMENT

Some functions may tolerate downtime; others cannot.



PLAN EARLY

Migration strategy belongs in system design.

Why I Ask It

Migration strategy should be part of system design. Some systems or services may tolerate planned downtime. Others may not.

Before developing a cutover plan, I want to know which functions the organization considers non-negotiable. Those answers influence phasing, redundancy, scheduling and how old and new systems may need to coexist.

DISCOVERY NOTE

Migration strategy should be part of system design.

22

Which locations can never lose security coverage?



PLACE MATTERS

System uptime and location coverage are different questions.



PROTECT CRITICAL AREAS

Sequence work around locations that must remain covered.

Why I Ask It

This is related to the previous question, but it is not the same. One asks about systems and services. This asks about physical locations.

Certain areas may require continuous coverage even if other parts of the property can tolerate temporary disruption. Understanding those locations early helps the team build migration sequencing around operational reality.

DISCOVERY NOTE

This is related to the previous question, but it is not the same.

23

Can the old and new systems operate simultaneously during migration?



COEXISTENCE HELPS

Large migrations are rarely one cutover.



PLAN THE PATH

Understand whether old and new systems can run together.

Why I Ask It

Large modernization projects are rarely completed in one cutover. The organization may need to operate the existing environment while portions of the new system come online.

I want to understand whether coexistence is technically and operationally possible.

KEY PRINCIPLE

The new system matters. So does the path from the old system to the new one.

24

What are the blackout dates, dark periods, offseason windows or other preferred work periods?



OPERATIONS SET THE WINDOW

The best technical plan must fit the real calendar.



USE THE QUIET PERIODS

Identify blackout dates and preferred work windows early.

Why I Ask It

Technical design is only part of a successful deployment. The project has to coexist with the organization's actual operations.

There may be major events, periods of peak occupancy, restricted work windows or times when large amounts of work can be completed with much less disruption.

KEY PRINCIPLE

A technically perfect deployment plan is not useful if the organization cannot operate around it.

25

Who has authority to approve the system as it comes online?



ACCEPT AS YOU GO

Waiting until the end creates avoidable rework.



NAME THE APPROVER

Clear decision authority keeps deployment moving.

Why I Ask It

Acceptance should happen throughout the project - not only at the end. For cameras, for example: as new cameras come online, who is responsible for approving the viewing angles?

The same principle applies to doors, integrations, workflows and other system behavior. Clear ownership allows questions to be resolved while work is happening instead of creating a large list of disagreements and rework at the end.

DISCOVERY NOTE

Acceptance should happen throughout the project - not only at the end.

GET THE RIGHT PEOPLE IN THE ROOM EARLY

One of the biggest roadblocks in complex projects usually is not the technology. It is assumptions. Security assumes IT is comfortable with the network. IT assumes Facilities has power and pathways covered. Facilities assumes Security has defined the operational requirements. Operations may not have been involved at all.

My preference is simple: get the right people in the room early and agree on the objective before anyone starts picking products.

FACILITIES	Understands how the building is constructed.
SECURITY	Understands the risks and operational requirements.
IT	Understands the infrastructure and cybersecurity.
OPERATIONS	Understands how people actually use the space.
LEADERSHIP	Understands business priorities, investment and long-term direction.

Bringing those perspectives together early reduces assumptions, prevents redesign and usually leads to a system the organization can actually support.

DISCOVERY BEFORE TECHNOLOGY

These questions are selected from a much larger discovery methodology. Every environment is different.

A stadium, corporate campus, healthcare facility, hospitality property, critical infrastructure site or multi-location enterprise will introduce different stakeholders, infrastructure, integrations and operating constraints.

The purpose of discovery is not to run through a checklist as quickly as possible. It is to uncover what matters, identify assumptions, expose dependencies, establish ownership and understand where the organization is going.

I would always rather spend a little longer asking questions at the beginning than spend months fixing assumptions later.

UNDERSTAND THE ENVIRONMENT.
UNDERSTAND THE OPERATIONS.
UNDERSTAND THE RISK.
THEN DESIGN THE TECHNOLOGY.

PLANNING A PHYSICAL SECURITY MODERNIZATION?

Start with discovery.

Use these questions to begin the conversation, challenge assumptions and identify the dependencies that should be understood before technology decisions are made.

ABOUT CRAIG BRUCE

Craig Bruce

Physical Security Executive & COO

Craig Bruce is a physical security executive and COO of Castaway Technology & Security (CTS). His work focuses on physical security, infrastructure modernization, business operations and complex security technology deployments.

[CraigBruce.com](https://craigbruce.com)